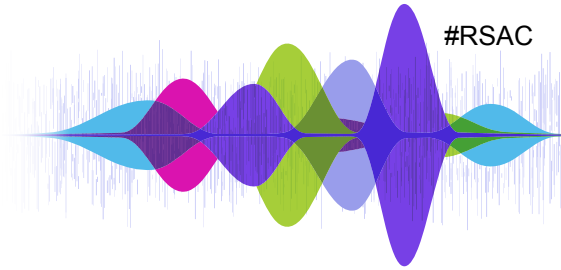
RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: APP-T10

ASPM & Hidden OSI Layer: Source Code

Kayra Otaner
Director of DevSecOps
Roche
https://www.linkedin.com/in/kayraotaner/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

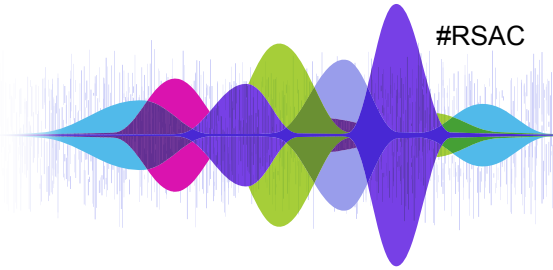
About me

Kayra Otaner

https://www.linkedin.com/in/kayraotaner

- Linux user since 1994
- Gentoo & Linux From Scratch User (#5893)
- Primarily in fin-tech space for last 15 years
- Director of DevSecOps at Roche
- Previously WPP, FICO, ADP
- Author of first Php & MySQL book written in Turkish published in 2001.
- Chief Architect for Turkish Navy's Cyber Security solution (www.ahtapot.org.tr) 2015
- Public speaker:
  - DevOpsDays Istanbul 2016
  - DevOpsPro Lithuania 2017
  - DevOpsPro Moscow 2017
  - DevOps Europe 2018 Lithua
  - DevSecOps Days 2019 Istar
  - DevSecOps Days Washingtc
  - KubeCon/CDSummit 2022 I
  - RSA 2023

ASPM & Hidden OSI Layer: Source Code

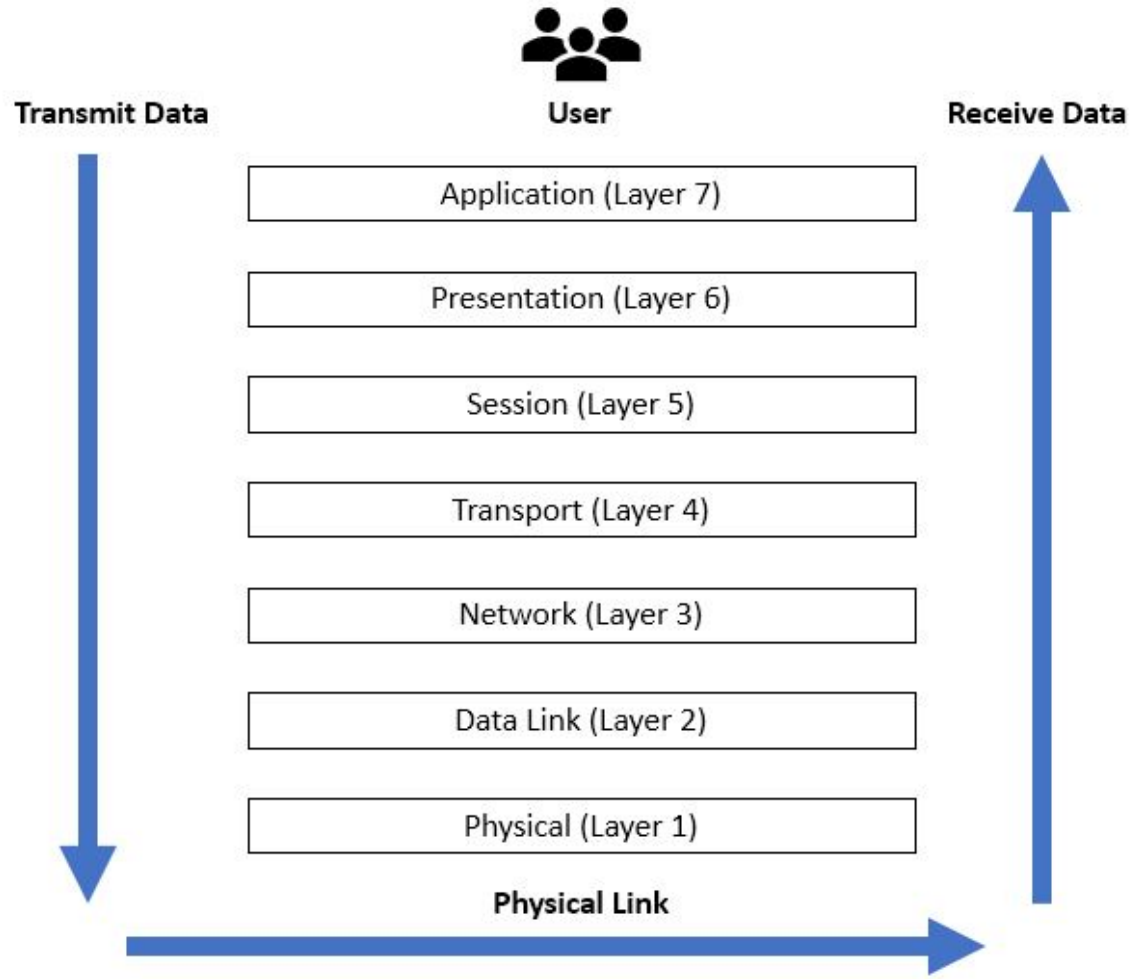


- What are the 7 layers of OSI Model?
- Layer 8?
- What is ASPM?
- 2024: Regulations, frameworks & Shifting Liability (CISA)
- SBOM, VEX, CSAF and Software Supply Chain
- How to quickly implement Application Security Posture Management?
- Software shelf life & last mile problems
- Bonus slides: Product Security vs Platform Security

RSAC | 2025 Conference

What are the 7 layers of OSI Model?

Layers of OSI Model



Wikipedia
The Free Encyclopedia

Search Wikipedia | Search

OSI model

73 languages

Article | Talk | Read | Edit | View history | Tools

From Wikipedia, the free encyclopedia

Contents hide

(Top)
History
Definitions
Standards documents
Layer architecture
Layer 1: Physical layer
Layer 2: Data link layer
Layer 3: Network layer
Layer 4: Transport layer
Layer 5: Session layer
Layer 6: Presentation layer
Layer 7: Application layer
Cross-layer functions
Programming interfaces
Comparison to other networking suites
Comparison with TCP/IP model
See also
References
Further reading
External links

OSI model
by layer

7. Application layer [show]
6. Presentation layer [show]
5. Session layer [show]
4. Transport layer [show]
3. Network layer [show]
2. Data link layer [show]
1. Physical layer [show]

v • t • e

The **Open Systems Interconnection** (**OSI**) **model** is a reference model developed by the International Organization for Standardization (ISO) that "provides a common basis for the coordination of standards development for the purpose of systems interconnection."[2]

In the OSI reference model, the components of a communication system are distinguished in seven abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.[3]

The model describes communications from the physical implementation of transmitting bits across a transmission medium to the highest-level representation of data of a distributed application. Each layer has well-defined functions and semantics and serves a class of functionality to the layer above it and is served by the layer below it. Established, well-known communication protocols are decomposed in software development into the model's hierarchy of function calls.

The Internet protocol suite as defined in RFC 1122 and RFC 1123 is a model of networking developed contemporarily to the OSI model, and was funded primarily by the U.S. Department of Defense. It was the foundation for the development of the Internet. It assumed the presence of generic physical links and focused primarily on the software layers of communication, with a similar but much less rigorous structure than the OSI model.

In comparison, several networking models have sought to create an intellectual framework for clarifying networking concepts and activities,[*citation needed*] but none have been as successful as the OSI reference model in becoming the standard model for discussing and teaching networking in the field of information technology. The model allows transparent communication through equivalent exchange of protocol data units (PDUs) between two parties, through what is known as peer-to-peer networking (also known as peer-to-peer communication). As a result, the OSI reference model has not only become an important piece among professionals and non-professionals alike, but also in all networking between one or many parties, due in large part to its commonly accepted user-friendly framework.[4]

Layer 8

"It's broken, I don't know how!"

WIKIPEDIA
The Free Encyclopedia

Search Wikipedia | Search

Layer 8

5 languages

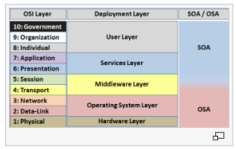
Article | Talk | Read | Edit | View history | Tools

Contents hide

(Top)
Layers, defined
Similar pseudo-layers for TCP/IP
Other uses
See also
References

From Wikipedia, the free encyclopedia

Layer 8 is a term used to refer to *user* or *political* layer on top of the 7-layer OSI model of computer networking.[1][2]



The OSI model is a 7-layer abstract model that describes an architecture of data communications for networked computers. The layers build upon each other, allowing for the abstraction of specific functions in each one. The top (7th) layer is the Application Layer describing methods and protocols of software applications. It is then held that the user is the 8th layer.

Layers, defined [edit]

According to Bruce Schneier and RSA:

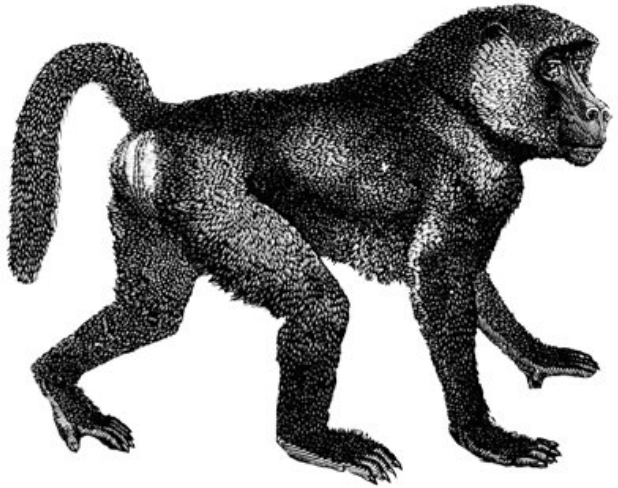
- Layer 8: The individual person.
- Layer 9: The organization.
- Layer 10: Government or legal compliance[3]

Network World readers[4] humorously report:

- Layer 8: Money - Provides network corruption by inspiring increased interference from the upper layer.
- Layer 9: Politics - Consists of technically ignorant management that negatively impacts network performance and development.

and:

- Layer 9: Politics. "Where the most difficult problems live."
- Layer 8: The user factor. "It turned out to be another Layer-8 problem."
- 7 to 1: The usual OSI layers
- Layer 0: Funding. "Because we should always start troubleshooting from the lowest layer, and nothing can exist before the funding."



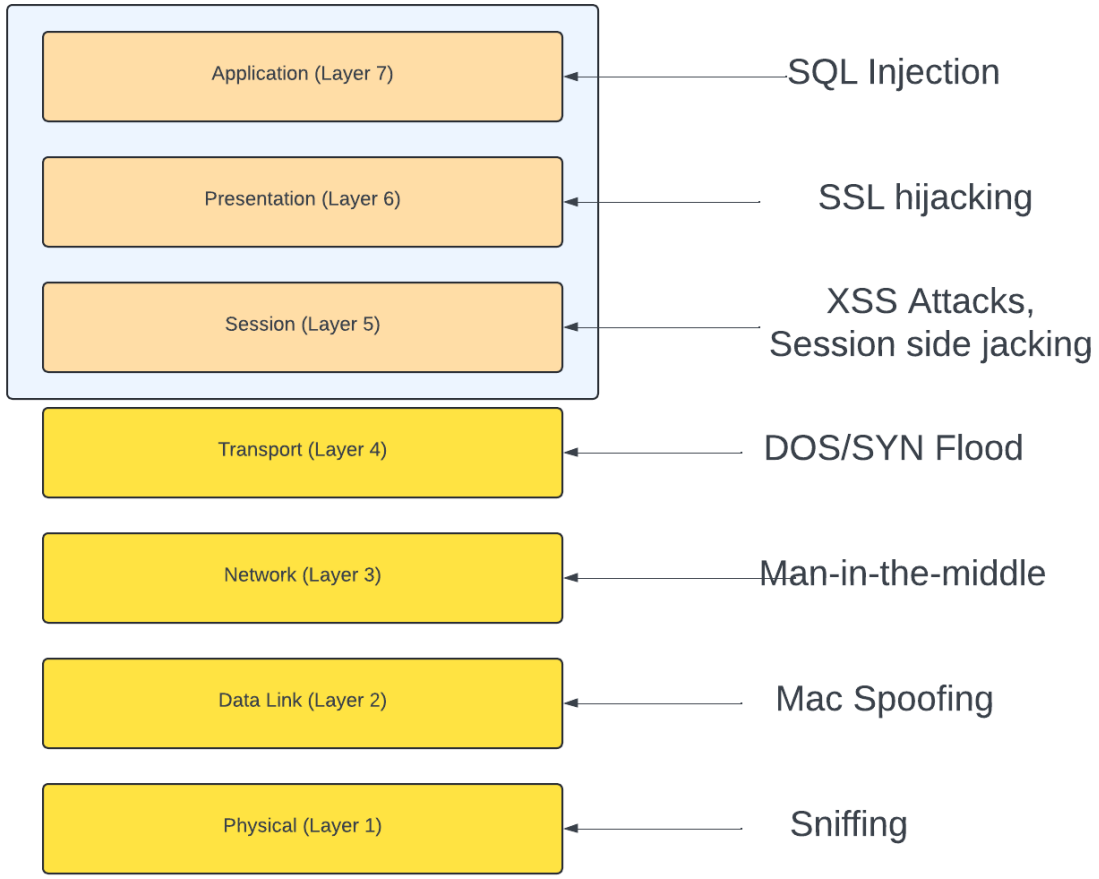
OSI Model
Layer 8

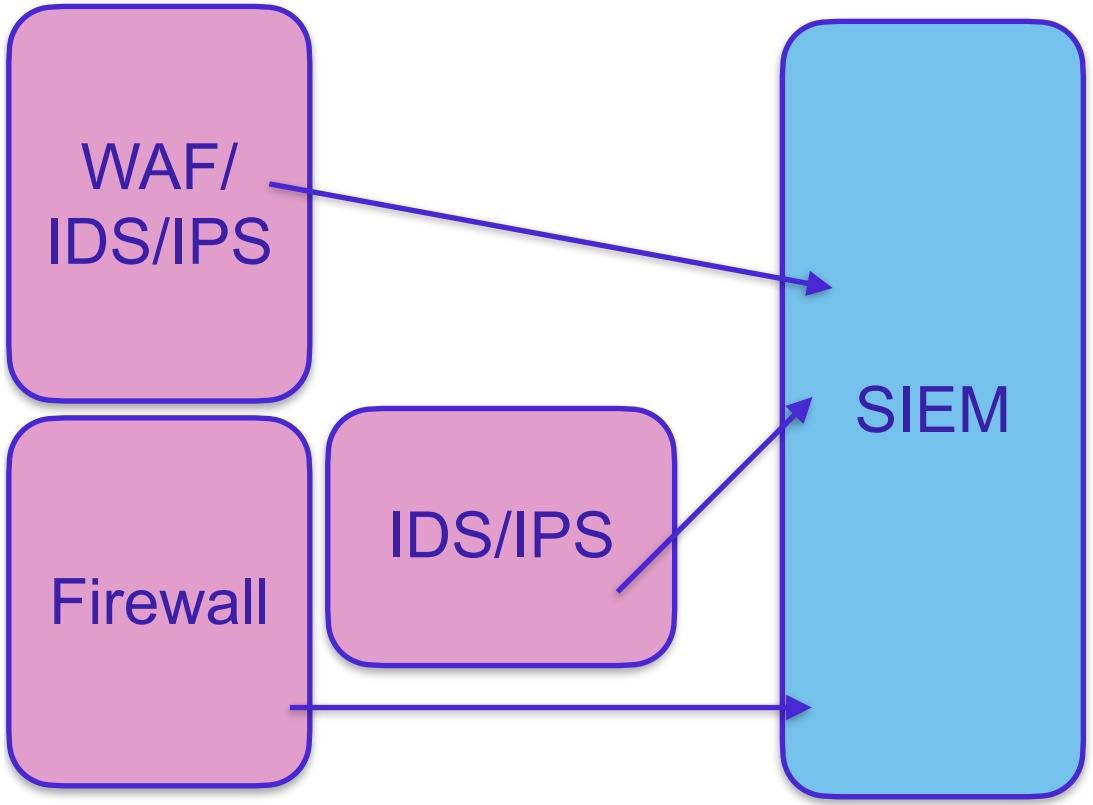
Identify the real problem

O RLY?

I. Amsuffering

OSI Model from security perspective





Verizon DBIR: 15% of the attacks

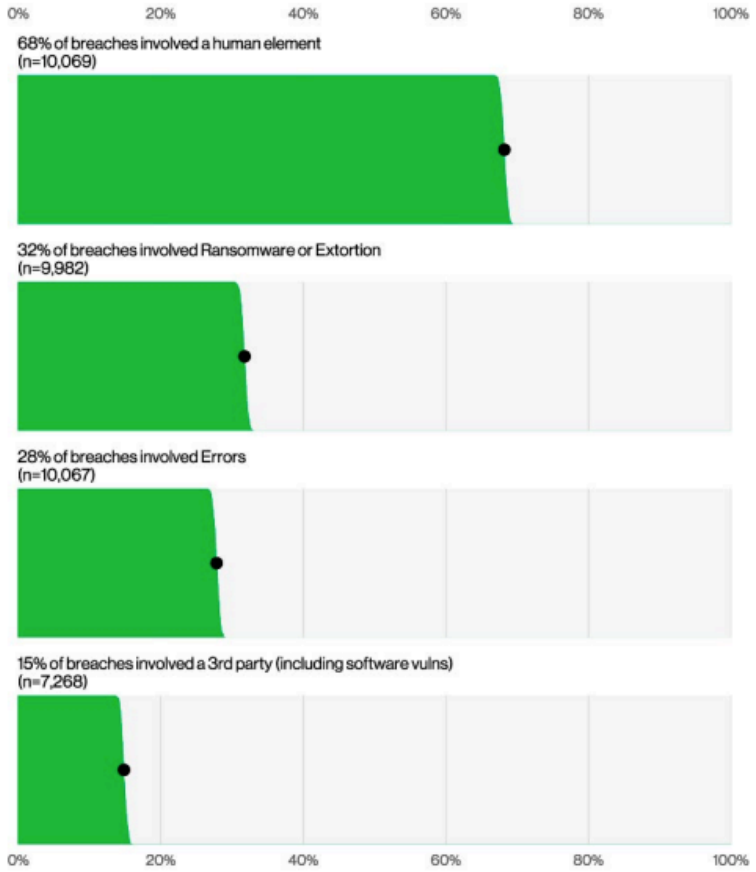


Figure 3. Select key enumerations in breaches

We have revised our calculation of the involvement of the human element to exclude malicious Privilege Misuse in an effort to provide a clearer metric of what security awareness can affect. For this year's dataset, the human element was a component of 68% of breaches, roughly the same as the previous period described in the 2023 DBIR.

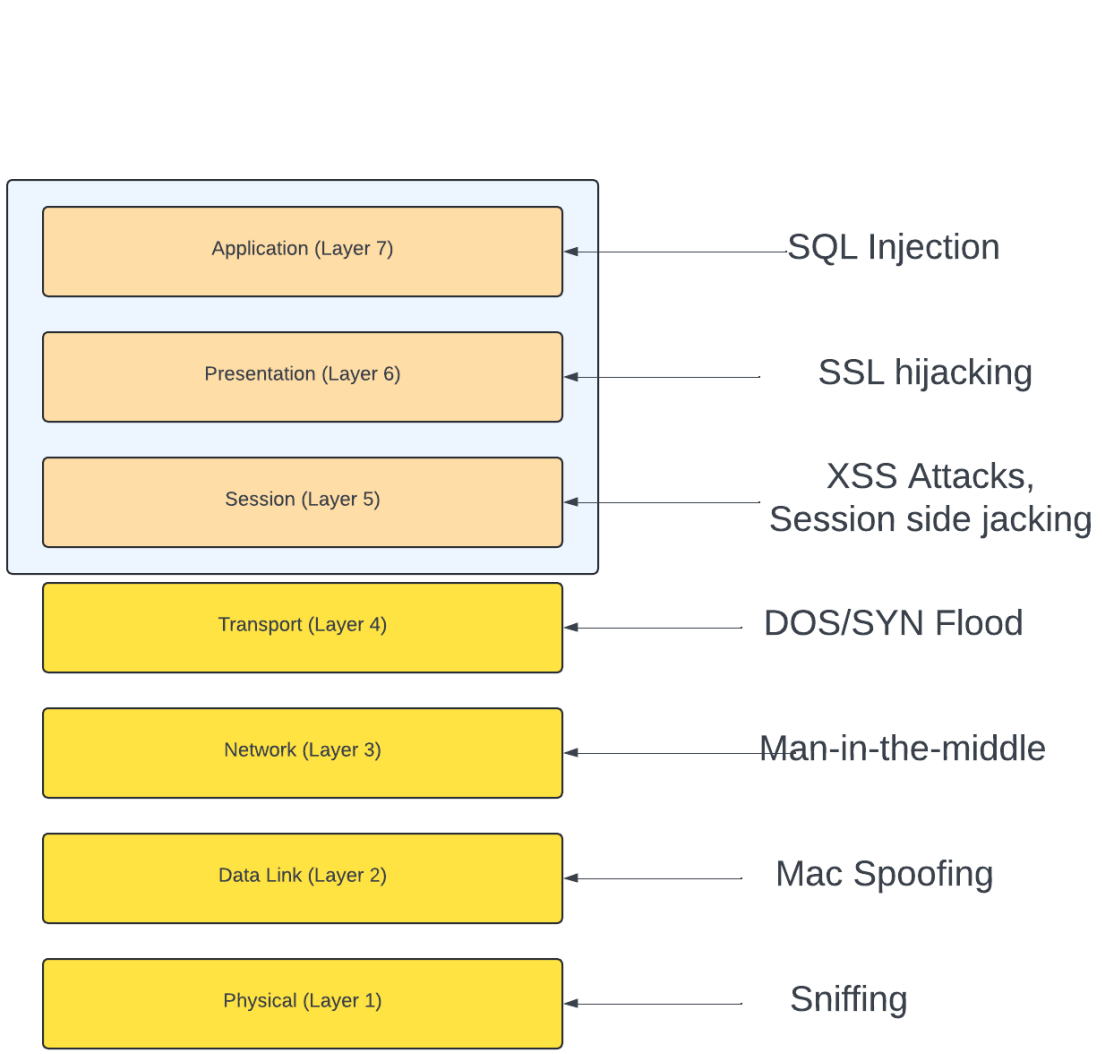
In this issue, we are introducing an expanded concept of a breach involving a third party that includes partner infrastructure being affected and direct or indirect software supply chain issues—including when an organization is affected by vulnerabilities in third-party software. In short, those are breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records. We see this figure at 15% this year, a 68% increase from the previous year, mostly fueled by the use of zero-day exploits for Ransomware and Extortion attacks.

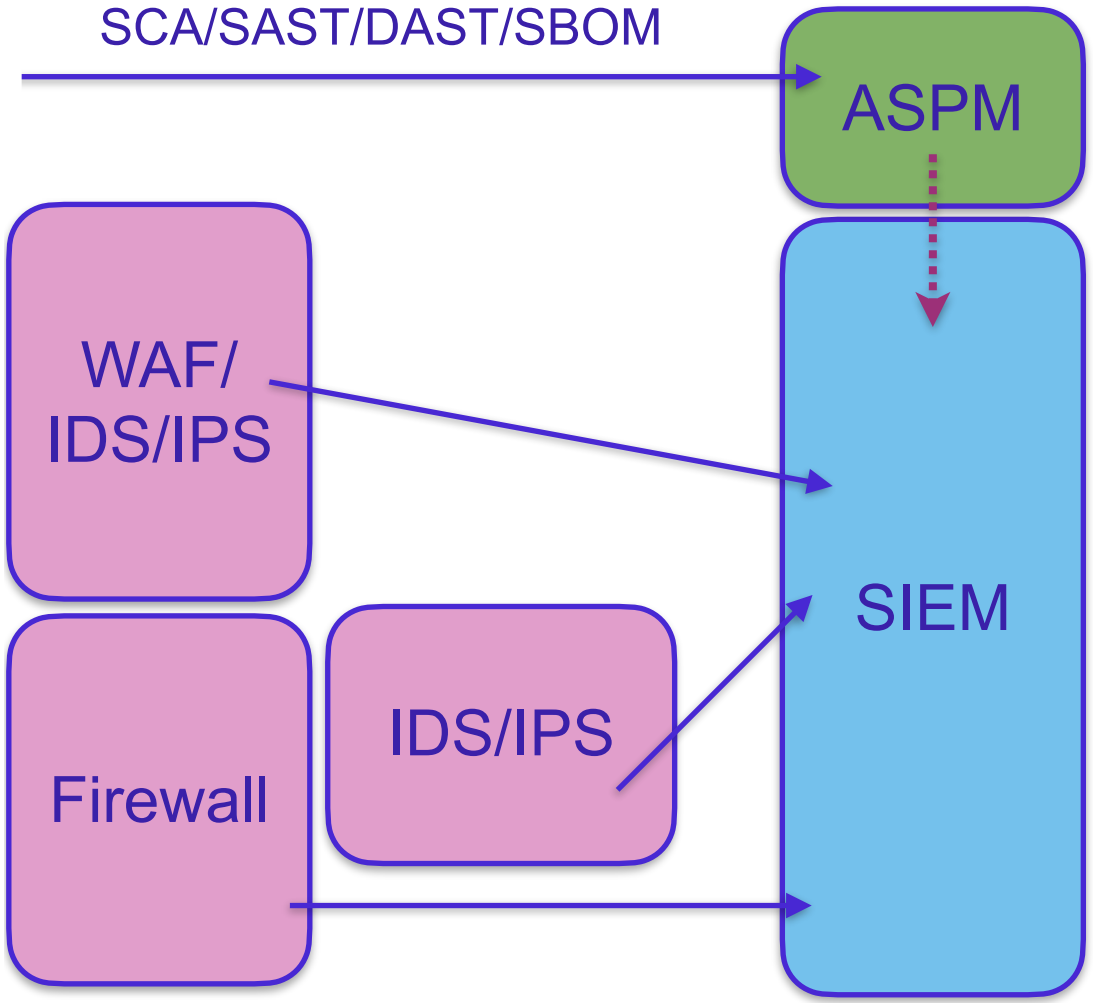
Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities. This validates our suspicion that errors are more prevalent than media or traditional incident response-driven bias would lead us to believe.

The 2024 Verizon DBIR found that breaches stemming from third-party software development organizations played a role in 15% of the more than 10,000 data breaches Verizon documented, a 68% jump from last year's report

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

OSI Model from security perspective





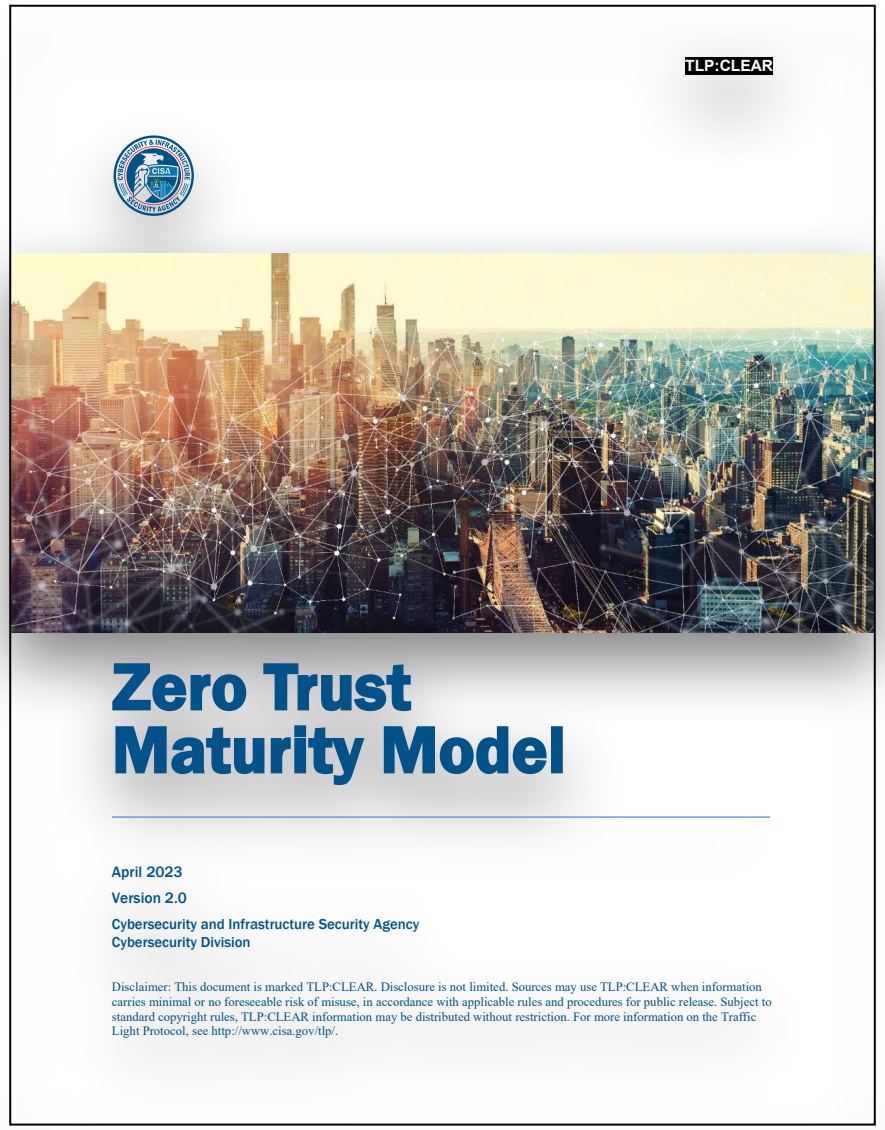
RSAC | 2025 Conference

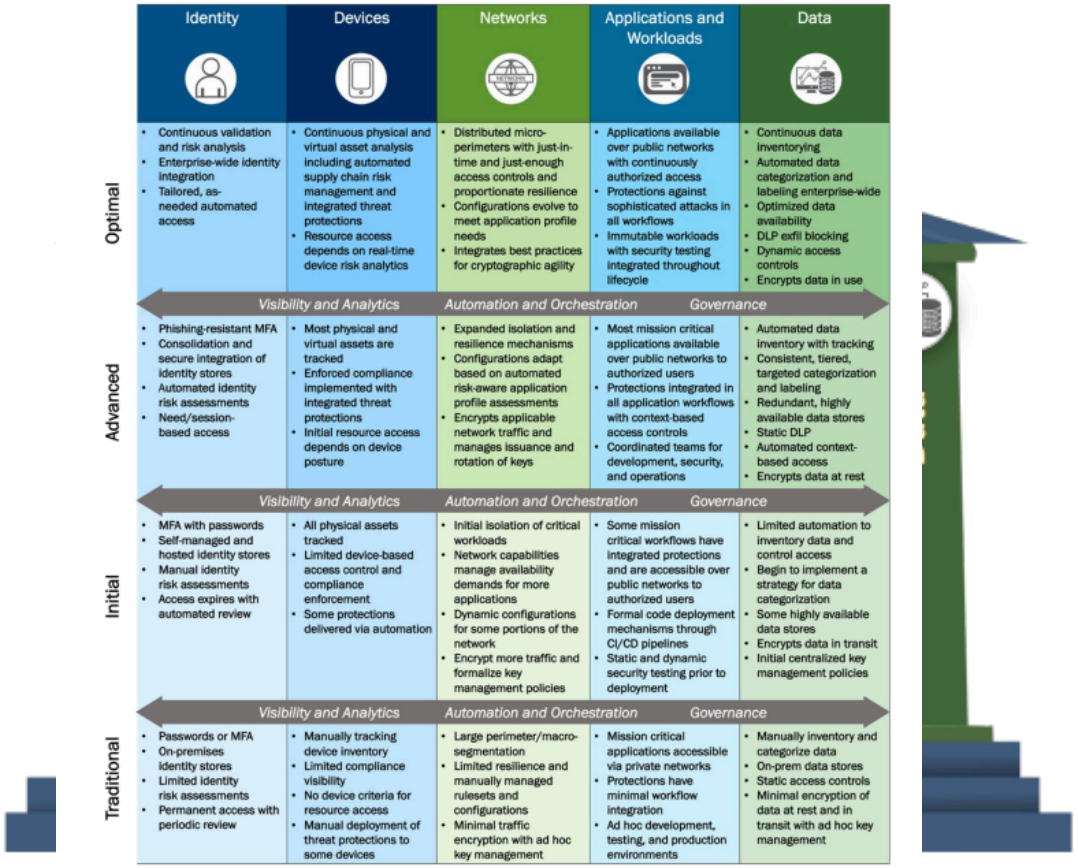
Why are we talking about ASPM in RSA 2025?

Regulations, frameworks and guidances that got published in 2023 & 2024

Many Voices.
One Community.

Zero Trust Maturity Model 2.0


TLP:CLEAR
Zero Trust Maturity Model
April 2023
Version 2.0
Cybersecurity and Infrastructure Security Agency
Cybersecurity Division
Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.



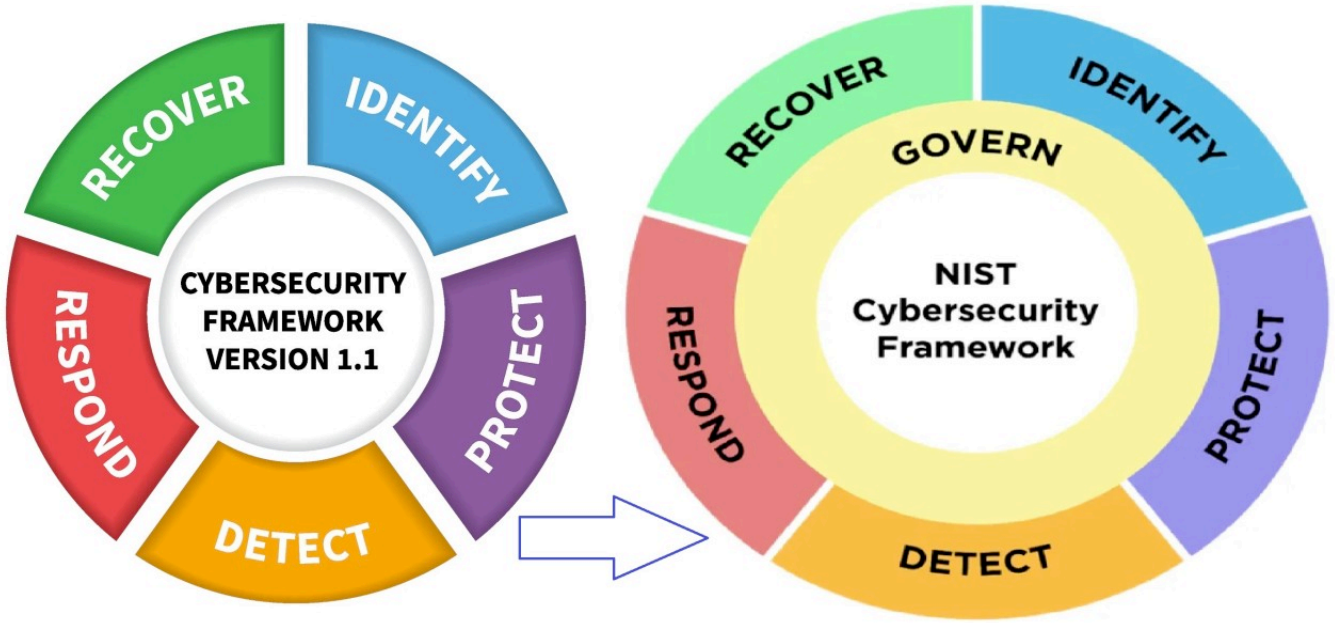
	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4: High-Level Zero Trust Maturity Model Overview

Agency implements tiered, tailored policies enterprisewide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.

https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

CSF 2.0 (February 2024)



The CSF Core Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — organize cybersecurity outcomes at their highest level.

- **GOVERN (GV)** — *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

Identify
- SBOM

Detect
- SAST
- DAST
- IAST

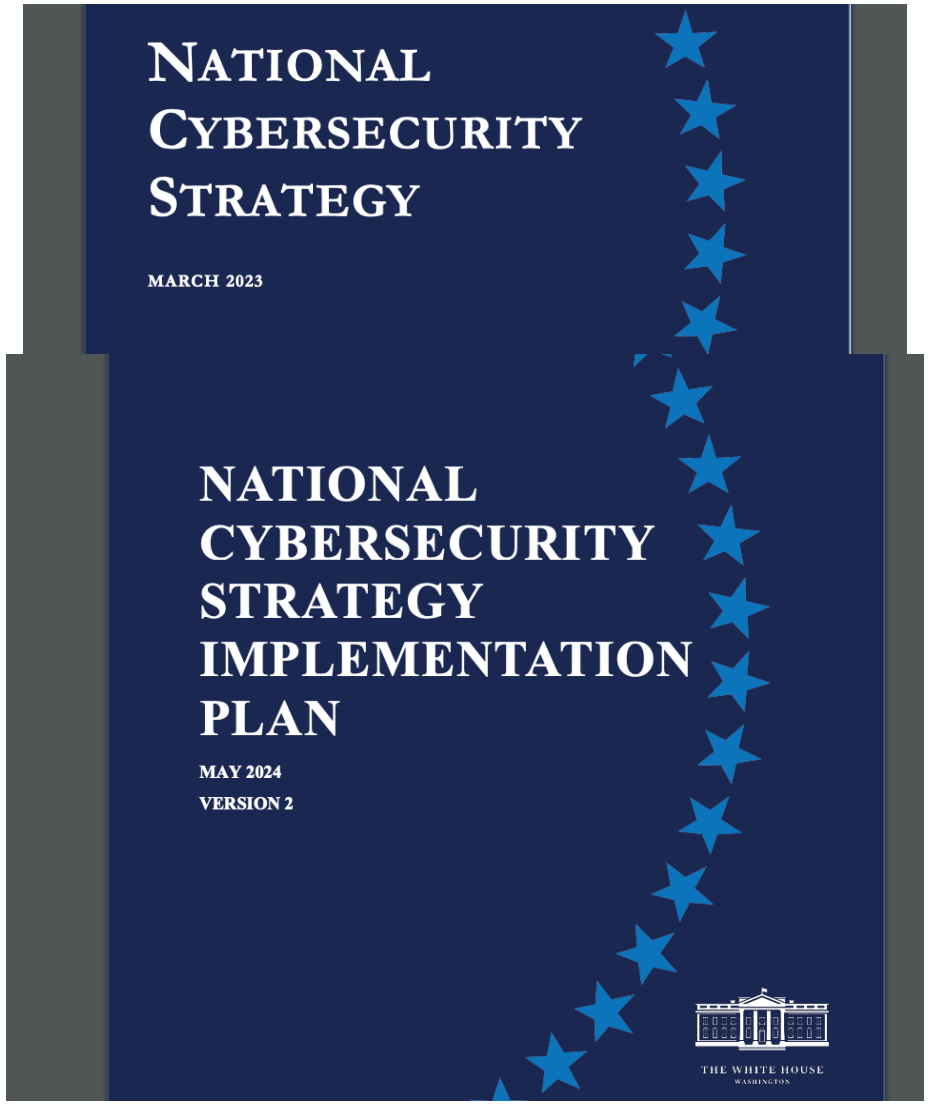
Respond/Remediate
- Manual

Protect/Prevent
- Supply Chain
- SLSA

Govern
- Security Posture Management
  - ASPM
  - CSPM

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Shifting Liability in 2Q 2025



Strategic Objective 3.3: Shift Liability for Insecure Software Products and Services

Initiative Number: *3.3.1*

Initiative Title: *Explore approaches to develop a long-term, flexible, and enduring software liability framework*

Initiative Number: 3.3.2

Initiative Title: Advance software bill of materials (SBOM) and mitigate the risk of unsupported software

Initiative Description

In order to collect data on the usage of unsupported software in critical infrastructure, the Cybersecurity and Infrastructure Security Agency will work with key stakeholders, including SRMAs, to identify and reduce gaps in SBOM scale and implementation. CISA will also explore requirements for a globally-accessible database for end-of-life/end-of-support software and convene an international staff-level working group on SBOM.

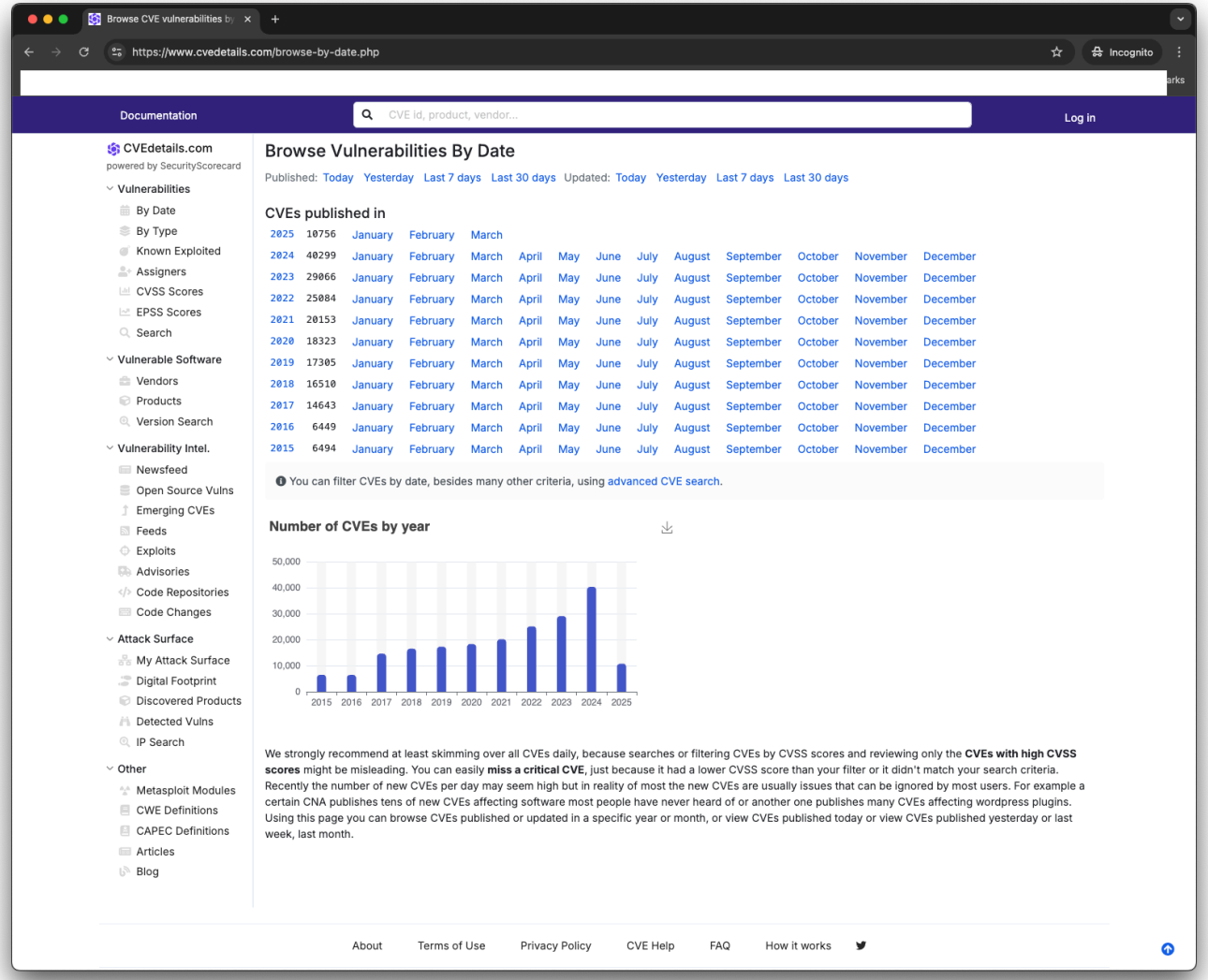
NCS Reference

…the Administration will .... promote the further development of SBOMs; and develop a process for identifying and mitigating the risk presented by unsupported software that is widely used or supports critical infrastructure.

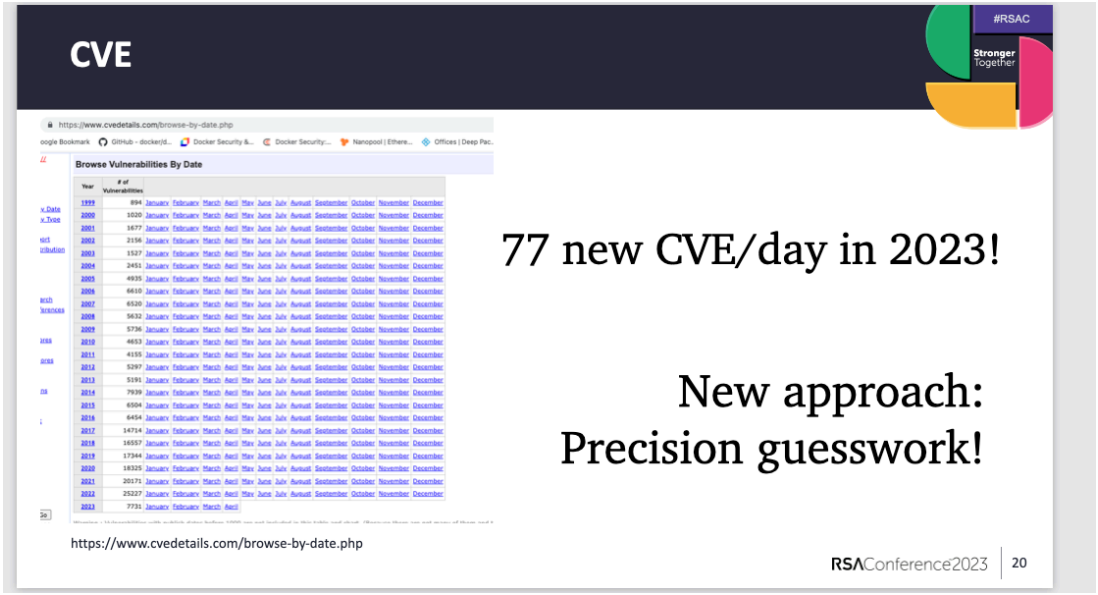
Responsible Agency: CISA

Completion Date: 2Q FY25

Explosion in CVE counts


Browse CVE vulnerabilities by
https://www.cvedetails.com/browse-by-date.php
Incognito
Documentation
CVE id, product, vendor...
Log in
CVEdetails.com
powered by SecurityScorecard
Vulnerabilities
By Date
By Type
Known Exploited
Assigners
CVSS Scores
EPSS Scores
Search
Vulnerable Software
Vendors
Products
Version Search
Vulnerability Intel.
Newsfeed
Open Source Vulns
Emerging CVEs
Feeds
Exploits
Advisories
Code Repositories
Code Changes
Attack Surface
My Attack Surface
Digital Footprint
Discovered Products
Detected Vulns
IP Search
Other
Metasploit Modules
CWE Definitions
CAPEC Definitions
Articles
Blog
Browse Vulnerabilities By Date
Published: Today Yesterday Last 7 days Last 30 days Updated: Today Yesterday Last 7 days Last 30 days
CVEs published in
2025 10756 January February March
2024 40299 January February March April May June July August September October November December
2023 29066 January February March April May June July August September October November December
2022 25084 January February March April May June July August September October November December
2021 20153 January February March April May June July August September October November December
2020 18323 January February March April May June July August September October November December
2019 17305 January February March April May June July August September October November December
2018 16510 January February March April May June July August September October November December
2017 14643 January February March April May June July August September October November December
2016 6449 January February March April May June July August September October November December
2015 6494 January February March April May June July August September October November December
You can filter CVEs by date, besides many other criteria, using advanced CVE search.
Number of CVEs by year
50,000
40,000
30,000
20,000
10,000
0
2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025
We strongly recommend at least skimming over all CVEs daily, because searches or filtering CVEs by CVSS scores and reviewing only the CVEs with high CVSS scores might be misleading. You can easily miss a critical CVE, just because it had a lower CVSS score than your filter or it didn't match your search criteria. Recently the number of new CVEs per day may seem high but in reality of most the new CVEs are usually issues that can be ignored by most users. For example a certain CNA publishes tens of new CVEs affecting software most people have never heard of or another one publishes many CVEs affecting wordpress plugins. Using this page you can browse CVEs published or updated in a specific year or month, or view CVEs published today or view CVEs published yesterday or last week, last month.
About Terms of Use Privacy Policy CVE Help FAQ How it works

2023: 79 CVE/day
2024: 110 CVE/day
2025: 130 CVE/day (as of 3/24/2025)

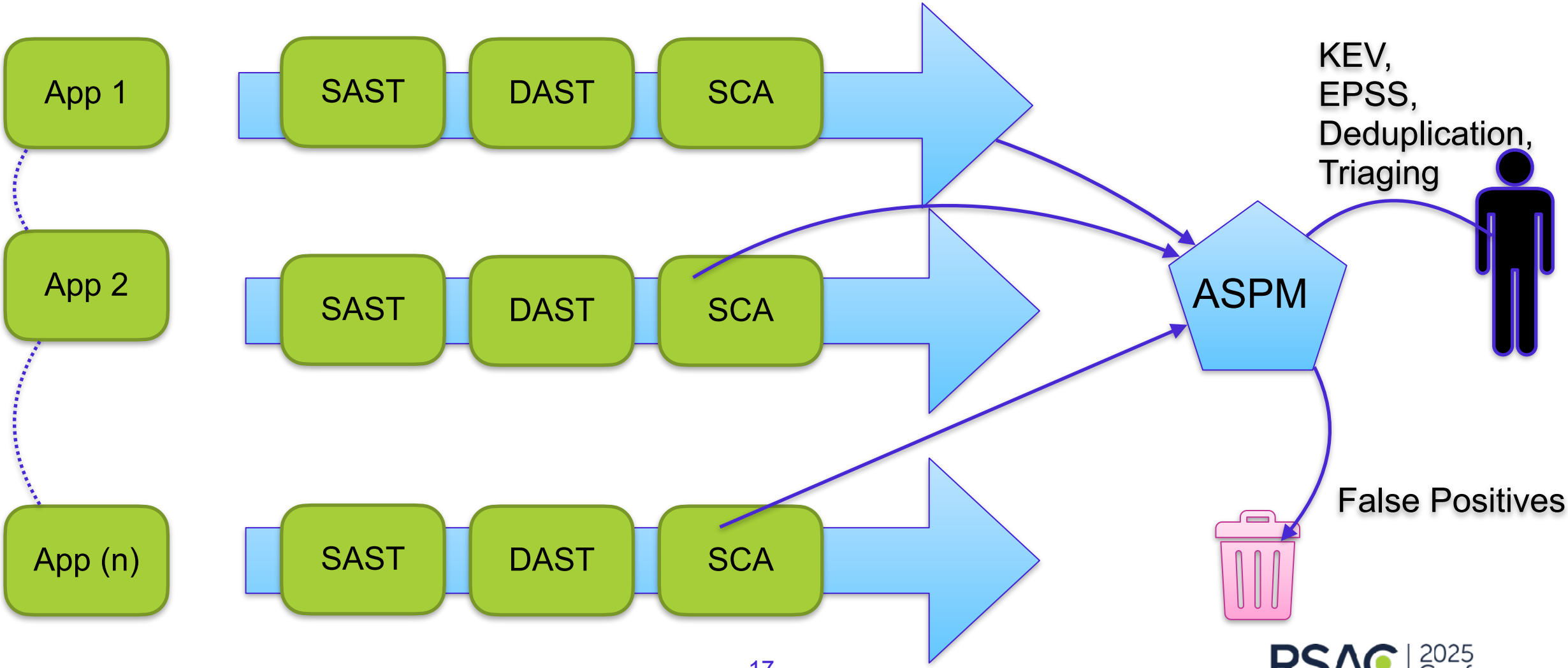


https://www.cvedetails.com/browse-by-date.php

Tool Sprawl

- You have products still in the market using legacy tool-stack
  - .Net Core 1.0
  - Borland Delphi 2006
  - Cobol
  - C/C++
  - Most modern security tools can not provide good coverage for these
- You work for megacorp and have M&A
  - They come with cloud native infra and use a SAST/DAST/SCA vendor you don't have yet (pick one Snyk/Endor/ Semgrep/Checkmarx etc)
- You have teams that like to use OSS and have OS security tools deployed already
  - They have Semgrep/Trivy/Grype/ Sonarqube etc

Increased adoption of Shifting left



2025 will be the year of ASPM

- April 2023: Zero Trust Maturity Model 2.0
  - *December 2023: FDA / 524B (Medical Device Space specific)*
- February 2024: Cybersecurity Framework 2.0: Governance function
- May 2024: CISA, shift liability for insecure software
- Deeper adoption of DevSecOps and shift-left practices, increased signal detection
- Explosion in CVE velocity
- Tool sprawl

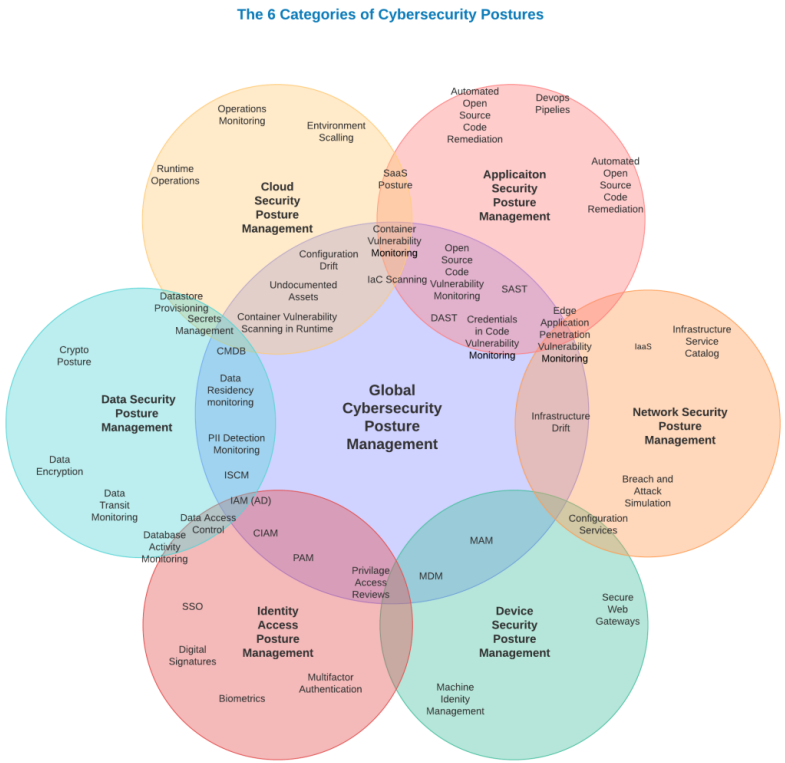
RSAC™ | 2025 Conference

What is ASPM?

Many Voices.
One Community.

Application Security Posture Management

According to google: ASPM term was coined by Gartner with their ASPM report published on May 2023



How to Build Your Cybersecurity Posture
6 Categories of Cybersecurity Posture
David Matousek
Cybersecurity Product Manager

6 Categories of Cybersecurity Posture

David Matousek
Engineering and Product Leader | Aligning Technology and Security outcomes to business objectives | Defining...

July 6, 2021

https://www.linkedin.com/pulse/6-categories-cybersecurity-posture-david-matousek/

Gartner ASPM Report

Gartner Information Technology Insights Expert Guidance Tools Connect with Peers

Gartner Research

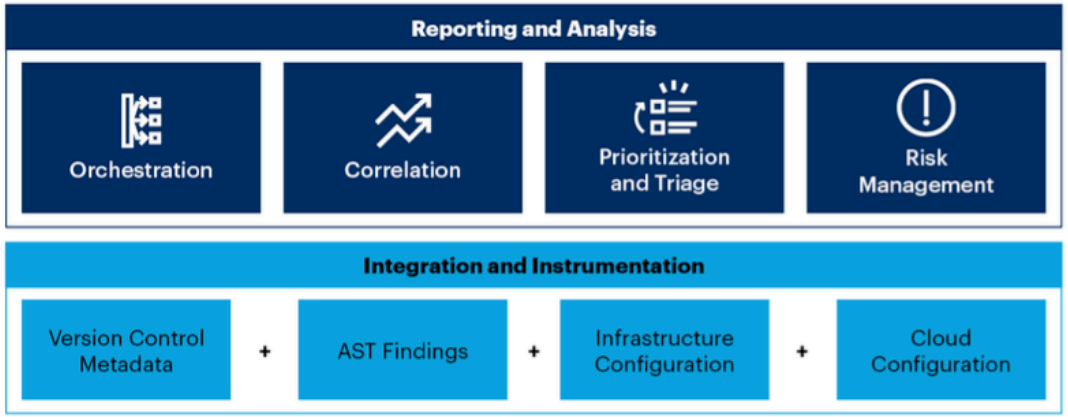
Innovation Insight for Application Security Posture Management

Published: 04 May 2023

Summary

Application security posture management analyzes security signals across software development, deployment and operation to improve visibility, better manage vulnerabilities and enforce controls. Security leaders can use ASPM to improve application security efficacy and better manage risk.

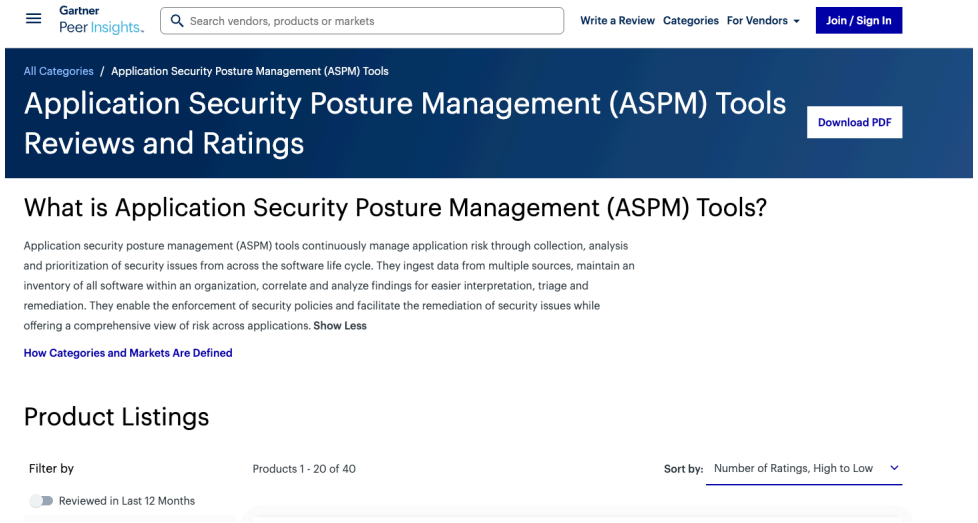
Application Security Posture Management

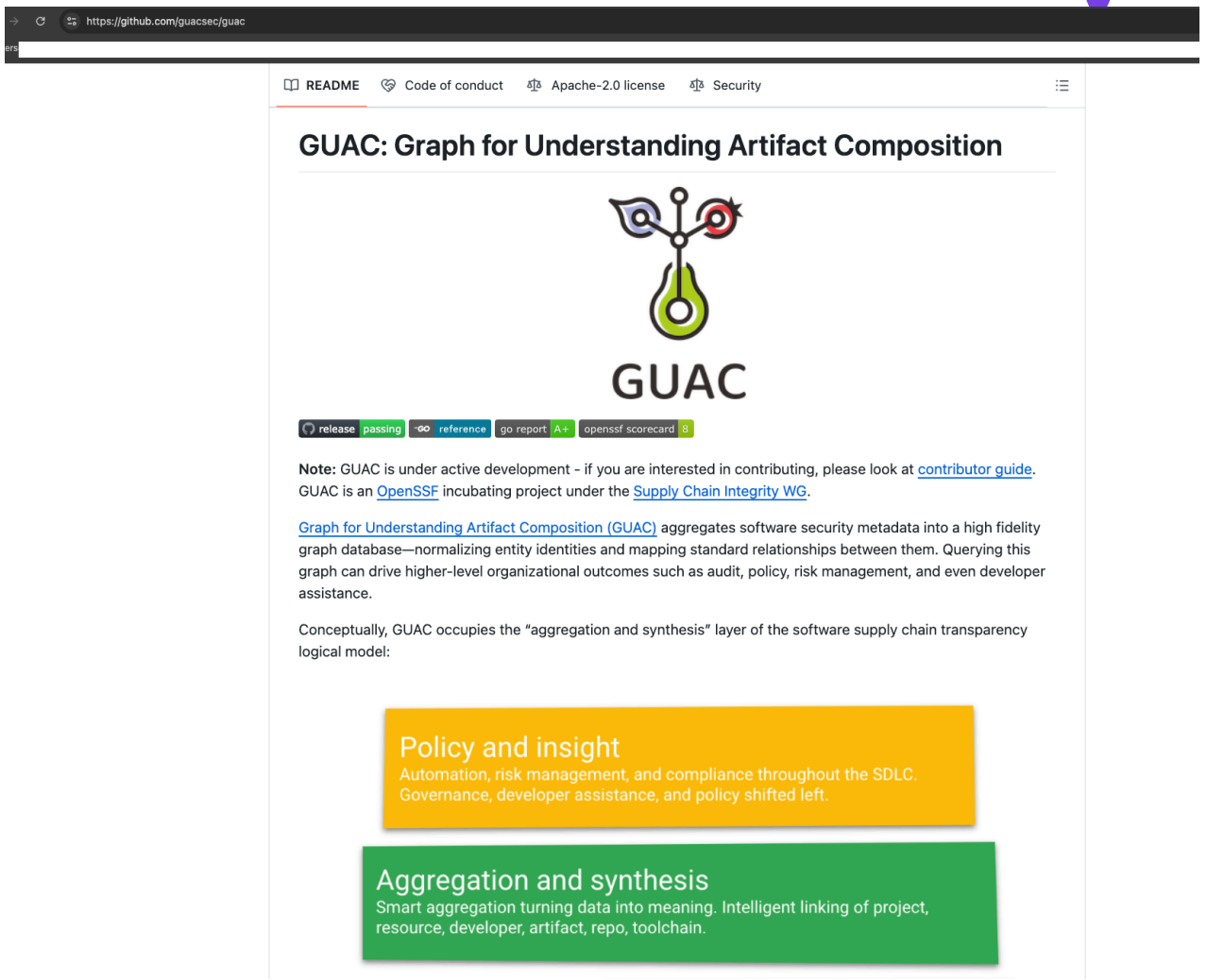


Source: Gartner
764962_C

https://www.gartner.com/en/documents/4326999

ASPM Solutions are still maturing


Gartner
Peer Insights.
Search vendors, products or markets
Write a Review
Categories
For Vendors
Join / Sign In
All Categories / Application Security Posture Management (ASPM) Tools
Application Security Posture Management (ASPM) Tools Reviews and Ratings
Download PDF
What is Application Security Posture Management (ASPM) Tools?
Application security posture management (ASPM) tools continuously manage application risk through collection, analysis and prioritization of security issues from across the software life cycle. They ingest data from multiple sources, maintain an inventory of all software within an organization, correlate and analyze findings for easier interpretation, triage and remediation. They enable the enforcement of security policies and facilitate the remediation of security issues while offering a comprehensive view of risk across applications. Show Less
How Categories and Markets Are Defined
Product Listings
Filter by
Products 1 - 20 of 40
Sort by:
Number of Ratings, High to Low
Reviewed in Last 12 Months


https://github.com/guacsec/guac
README
Code of conduct
Apache-2.0 license
Security
GUAC: Graph for Understanding Artifact Composition
GUAC
release passing
reference
go report A+
openssf scorecard 8
Note: GUAC is under active development - if you are interested in contributing, please look at contributor guide.
GUAC is an OpenSSF incubating project under the Supply Chain Integrity WG.
Graph for Understanding Artifact Composition (GUAC) aggregates software security metadata into a high fidelity graph database—normalizing entity identities and mapping standard relationships between them. Querying this graph can drive higher-level organizational outcomes such as audit, policy, risk management, and even developer assistance.
Conceptually, GUAC occupies the "aggregation and synthesis" layer of the software supply chain transparency logical model:
Policy and insight
Automation, risk management, and compliance throughout the SDLC.
Governance, developer assistance, and policy shifted left.
Aggregation and synthesis
Smart aggregation turning data into meaning. Intelligent linking of project,
resource, developer, artifact, repo, toolchain.

https://www.gartner.com/reviews/market/application-security-posture-management-aspm-tools

RSAC | 2025 Conference

SBOM & VEX

BomOps & Software Asset Management

Many Voices.
One Community.

SBOM

Dave Luber
@NSA_CSDirector
We are on the journey to SBOM. Want to know why we need it and how it will help? Good podcast with @cisagov @allanfriedman explaining it here!
youtu.be/s0VSJDLdxM4
SBOM
POTENTIAL BLOWS MY MIND
6:18 AM · Oct 18, 2022

Department of Commerce
The Minimum Elements for an SBOM

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

- The Minimum Elements For a Software Bill of Materials (SBOM)
- Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity
- July 12, 2021

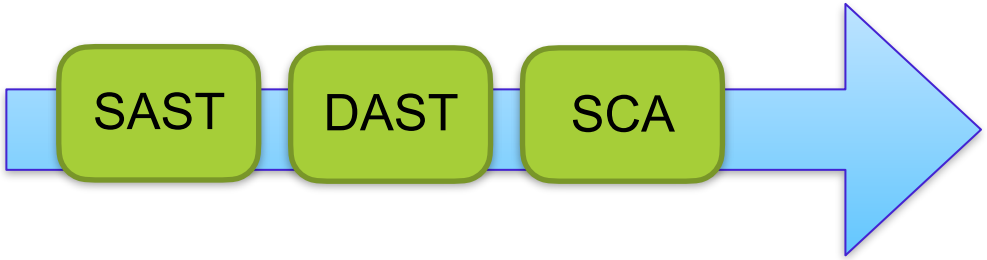
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

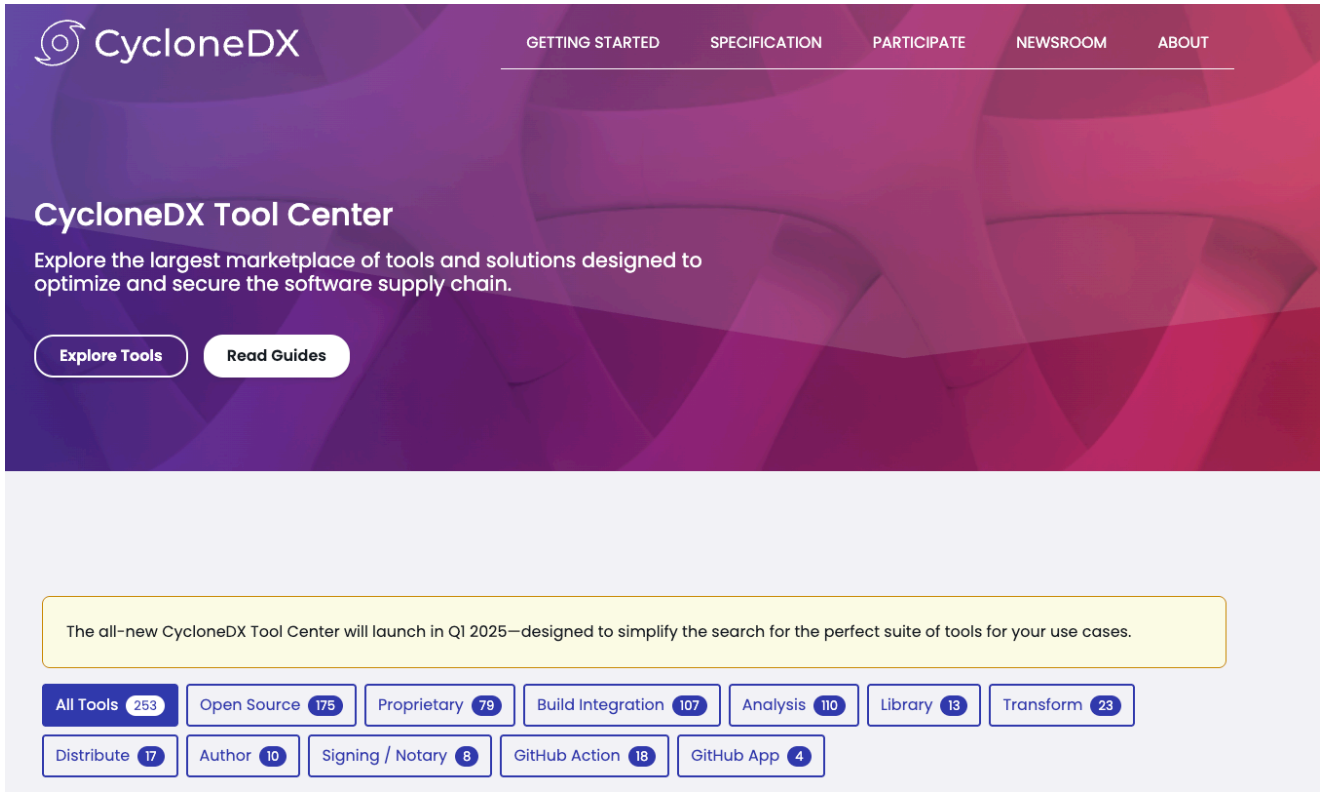
SBOM Elements and Considerations

"Operational considerations touch on when and where the SBOM data is generated and tracked. SBOM data could be created and stored in the repository of the source.

For built software, it can be tracked and assembled at the time of build.

A new build or an update to the underlying source should, in turn, create a new SBOM."





https://www.federalregister.gov/documents/2021/06/02/2021-11592/software-bill-of-materials-elements-and-considerations

SBOM, but how??

Buildpacks.io

Features

Advanced Caching

Robust caching is used to improve performance.

Bill-of-Materials

Insights into the contents of the app image through standard build-time SBOMs in CycloneDX, SPDX and Syft JSON formats.

README | Code of conduct | Apache-2.0 license | Security

CycloneDX Maven Plugin

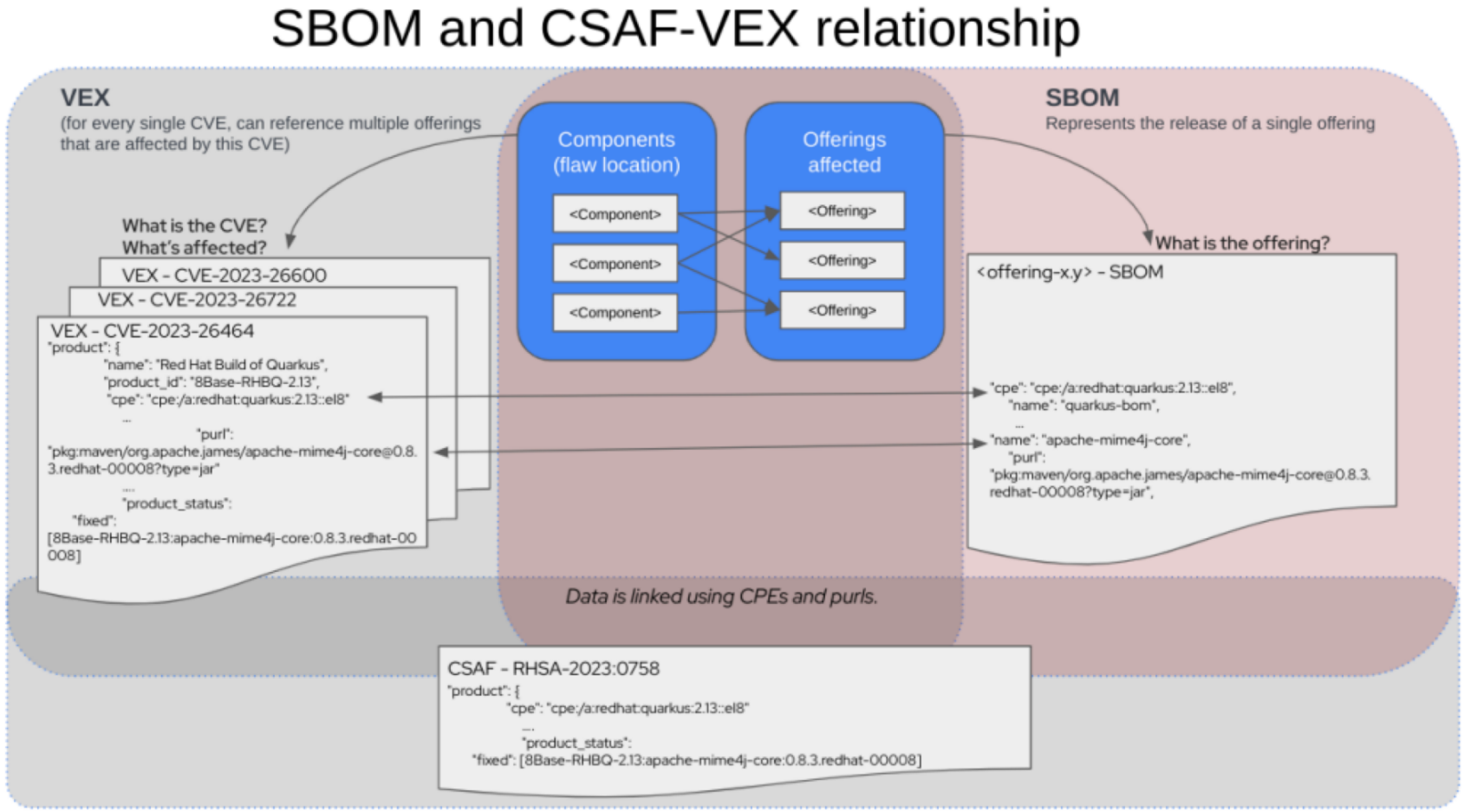
The CycloneDX Maven plugin generates CycloneDX Software Bill of Materials (SBOM) containing the aggregate of all direct and transitive dependencies of a project. CycloneDX is a full-stack SBOM standard designed for use in application security contexts and supply chain component analysis.

Maven Usage

```
<!-- uses default configuration -->
<plugins>
    <plugin>
        <groupId>org.cyclonedx</groupId>
        <artifactId>cyclonedx-maven-plugin</artifactId>
        <executions>
            <execution>
                <phase>package</phase>
                <goals>
                    <goal>makeAggregateBom</goal>
                </goals>
            </execution>
        </executions>
    </plugin>
</plugins>
```

Default Values

CSAF & VEX

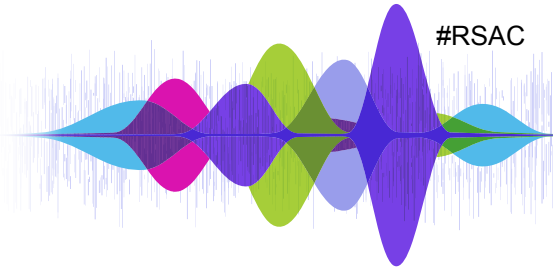


https://www.first.org/resources/papers/FIRSTPSIRT22/FIRST-PSIRT-TC-2022-OMAR-SANTOS.pdf

RSAC | 2025 Conference

How to establish ASPM

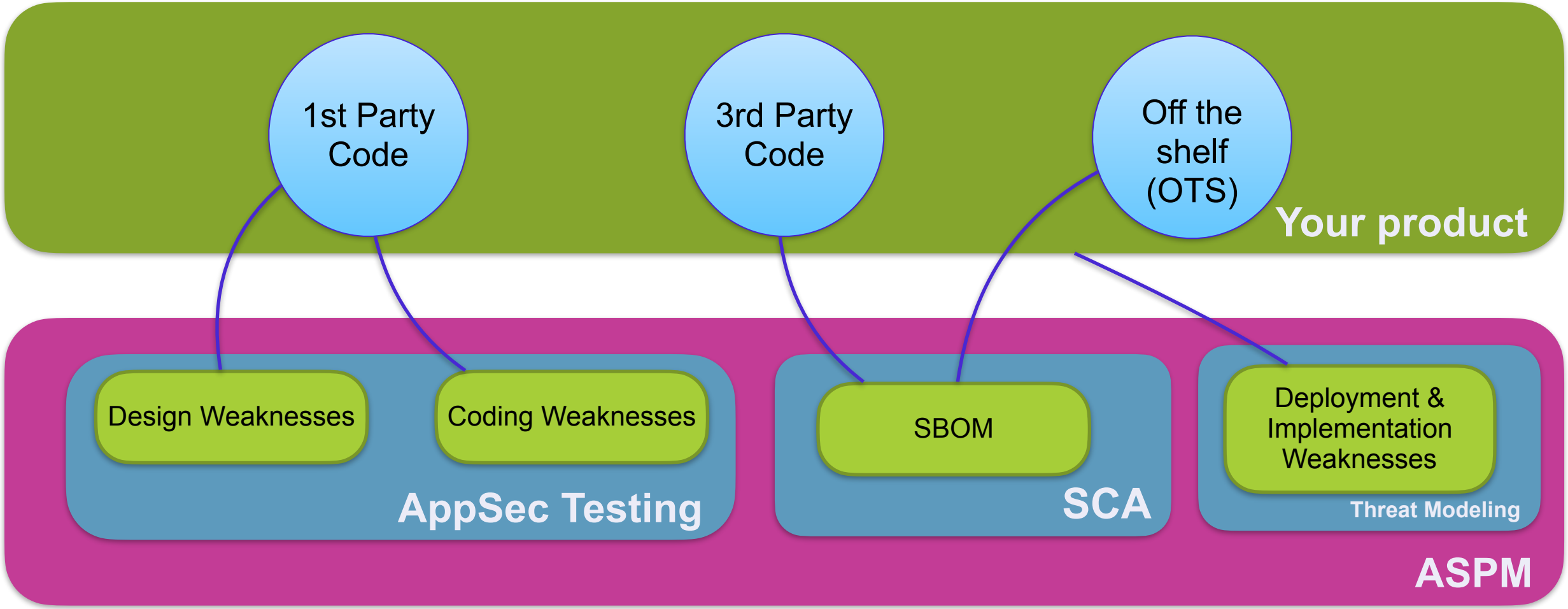
With Open Source Tools & KEV/EPSS 4.0



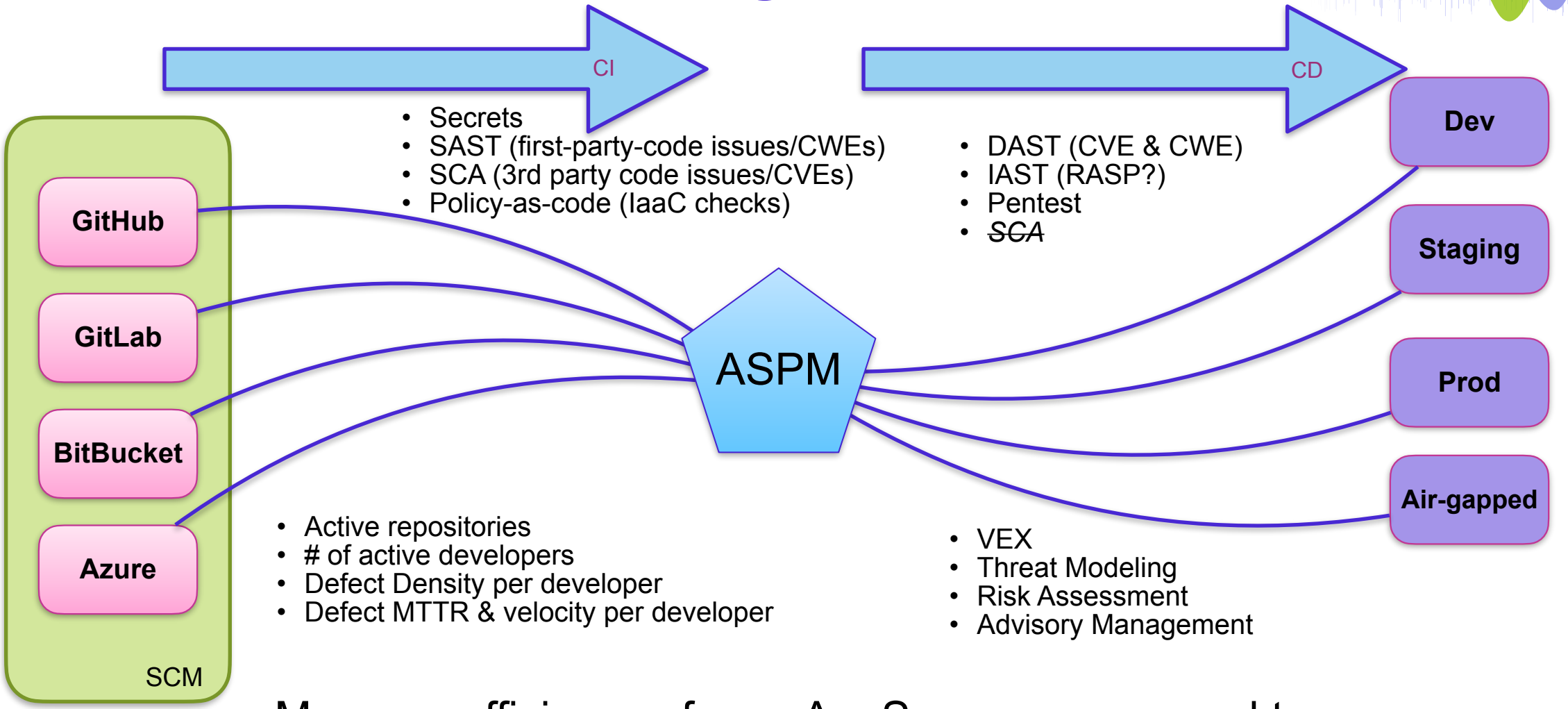
How to steps

- Discover
  - Collect all signals from all DevSecOps infrastructure
- Identify
  - Aggregate and deduplicate issues by CVE & CWE
  - Track issues by developer/repository/application
- Triage
  - Use threat modeling
  - Use EPSS
  - Adopt VEX & CSAF

ASPM & your product

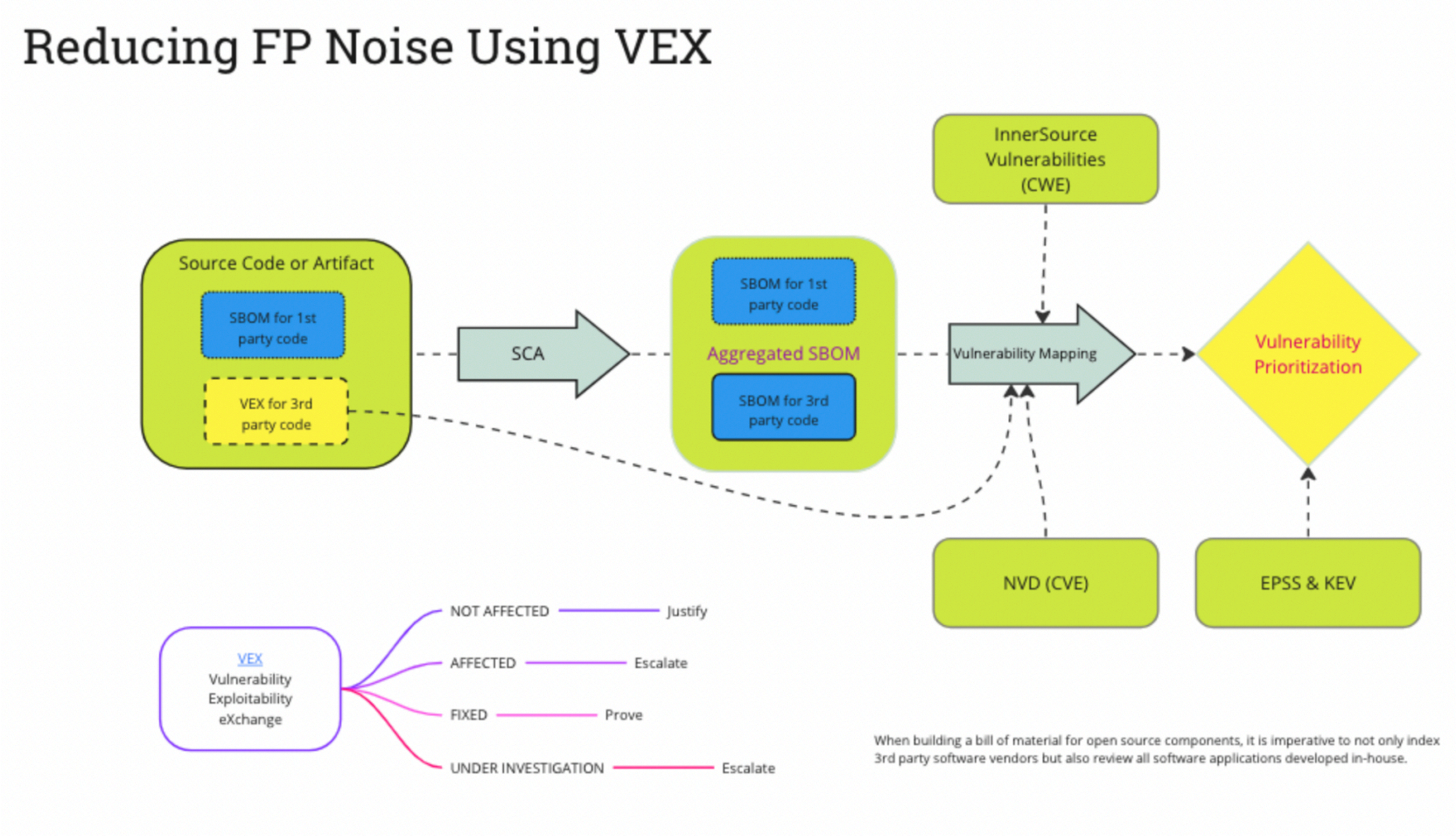


Connect & collect all signals



Measure efficiency of your AppSec processes and teams

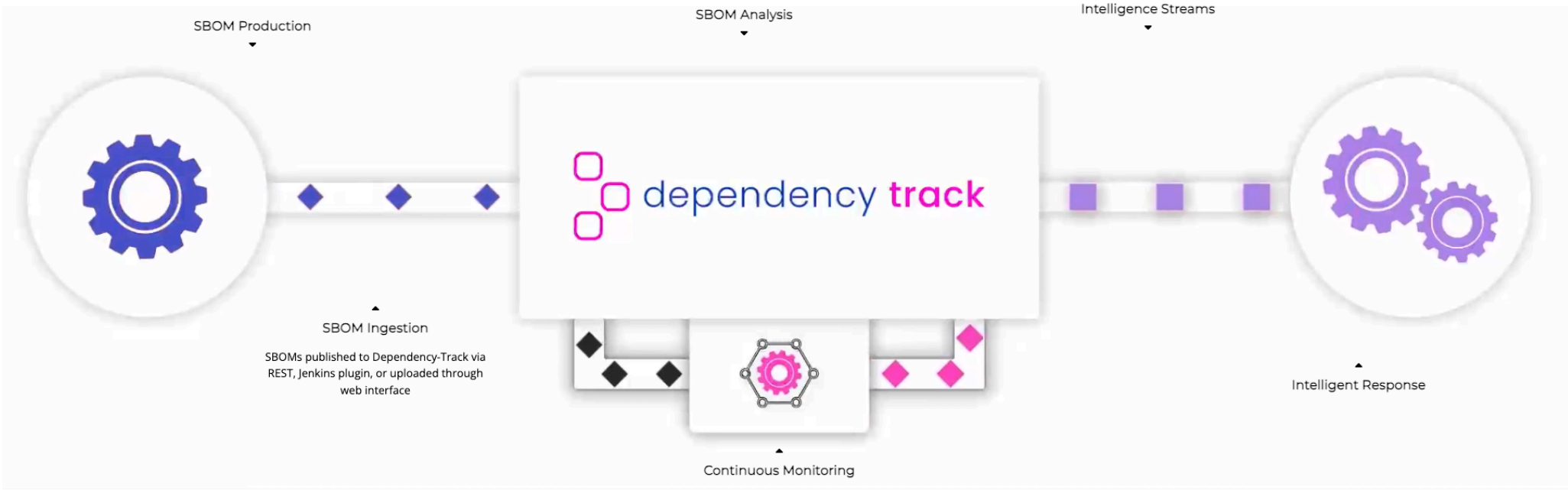
Use VEX & EPSS for triaging



SBOM: 3rd Party Code + Binary

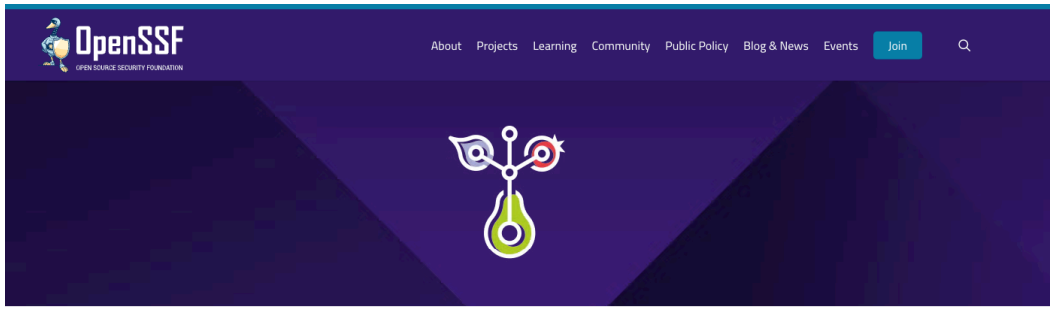
Deploy Dependency Track from OWASP

Operationalize Software Bill of Materials



SBOM: 3rd Party Code + Binary

Graph for Understanding Artifact Composition



Graph for Understanding Artifact Composition

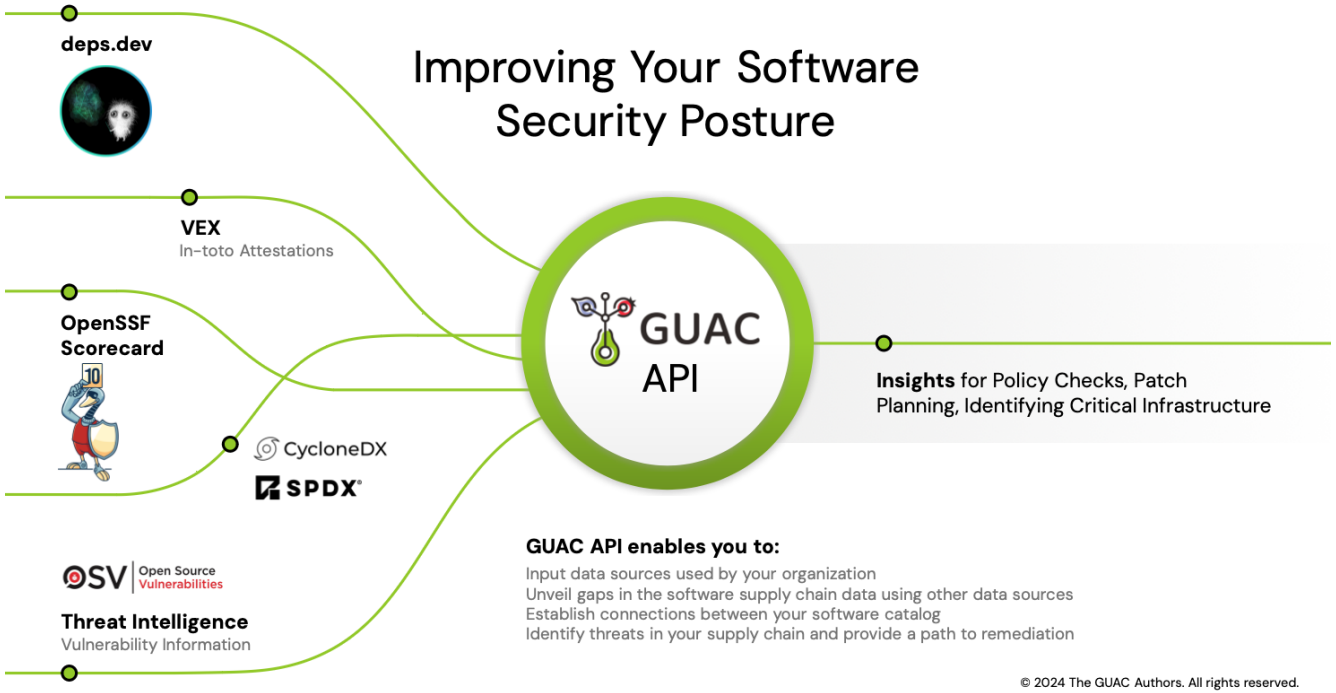
Software supply chain attacks are on the rise and it's hard to know what your software is at risk for and how to protect it. Many tools are available to help you generate Software Bills of Materials (SBOMs), signed attestations, and vulnerability reports, but they stop there, leaving you to figure out how they all fit together.

Our Vision

GUAC (Graph for Understanding Artifact Composition) aims to fill in the gaps by ingesting software metadata, like SBOMs, and mapping out relationships between software. When you know how one piece of software affects another, you'll be able to fully understand your software security position and act as needed.

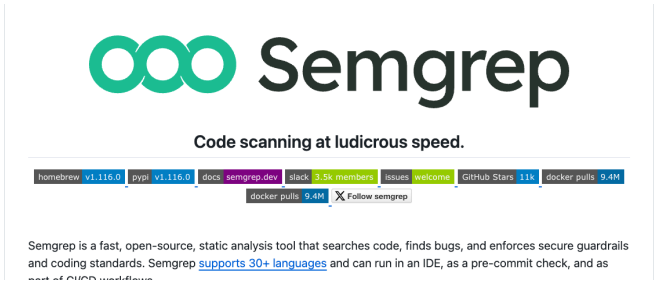
How can GUAC help you?

- **Proactive** Find the most used critical components in a software supply chain ecosystem
- **Operational** Determine weaknesses in overall security posture
- **Responsive** Prevent software supply chain compromises before they happen

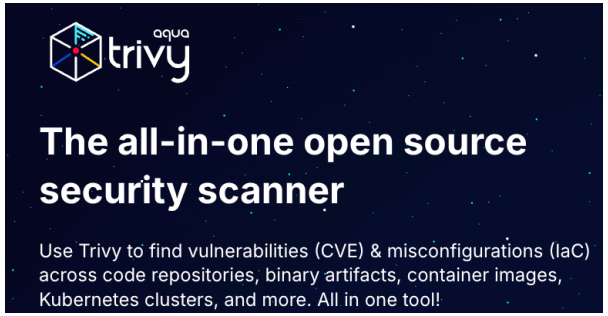

Improving Your Software Security Posture
deps.dev
VEX
In-toto Attestations
OpenSSF Scorecard
CycloneDX
SPDX
OSV Open Source Vulnerabilities
Threat Intelligence
Vulnerability Information
GUAC API
Insights for Policy Checks, Patch Planning, Identifying Critical Infrastructure
GUAC API enables you to:
Input data sources used by your organization
Unveil gaps in the software supply chain data using other data sources
Establish connections between your software catalog
Identify threats in your supply chain and provide a path to remediation
© 2024 The GUAC Authors. All rights reserved.

SAST & DAST

Quantity has a quality all its own. Aggregate & deduplicate findings


Semgrep
Code scanning at ludicrous speed.
homebrew v1.116.0
pypi v1.116.0
docs semgrep.dev
slack 3.5k members
issues welcome
GitHub Stars 11k
docker pulls 9.4M
docker pulls 9.4M
Follow semgrep
Semgrep is a fast, open-source, static analysis tool that searches code, finds bugs, and enforces secure guardrails and coding standards. Semgrep supports 30+ languages and can run in an IDE, as a pre-commit check, and as

grype
A vulnerability scanner for container images and filesystems. Easily install the binary to try it out. Works with Syft, the powerful SBOM (software bill of materials) tool for container images and filesystems.


aqua trivy
The all-in-one open source security scanner
Use Trivy to find vulnerabilities (CVE) & misconfigurations (IaC) across code repositories, binary artifacts, container images, Kubernetes clusters, and more. All in one tool!

- Most of them are already available in GitLab Open Source

Vulnerability scanner maintenance

Tier: Free, Premium, Ultimate
Offering: GitLab.com, GitLab Self-Managed, GitLab Dedicated

The following vulnerability scanners and their databases are regularly updated:

Secure scanning tool	Vulnerabilities database updates
Container Scanning	A job runs on a daily basis to build new images with the latest vulnerability database updates from the upstream scanner. GitLab monitors this job through an internal alert that tells the engineering team when the database becomes more than 48 hours old. For more information, see the Vulnerabilities database update.
Dependency Scanning	Relies on the GitLab Advisory Database which is updated on a daily basis using data from the National Vulnerability Database (NVD) and the GitHub Advisory Database.
Dynamic Application Security Testing (DAST)	DAST analyzer is updated on a periodic basis.
Secret Detection	GitLab maintains the detection rules and accepts community contributions. The scanning engine is updated at least once per month if a relevant update is available.
Static Application Security Testing (SAST)	The source of scan rules depends on which analyzer is used for each supported programming language. GitLab maintains a ruleset for the Semgrep-based analyzer and updates it regularly based on internal research and user feedback. For other analyzers, the ruleset is sourced from the upstream open-source scanner. Each analyzer is updated at least once per month if a relevant update is available.

AppSec Results

Deploy Defect Dojo

DEFECTDOJO

Platform Integrations Pricing Resources Company

The DevSecOps platform built for security teams

Import Scan Results
Import the results of various security scans, such as static code analysis (SAST), dynamic application security testing (DAST), software composition analysis (SCA) and other security tools.

Vulnerability Tracking
Manage and prioritize identified vulnerabilities for remediation.

Metrics And Reporting
Understand security trends with detailed metrics and reports.

Integration With Testing Tools
Integrate with over 180+ security testing tools and platforms.

Risk Scoring And Prioritization
Score and prioritize vulnerabilities based on impact and risk.

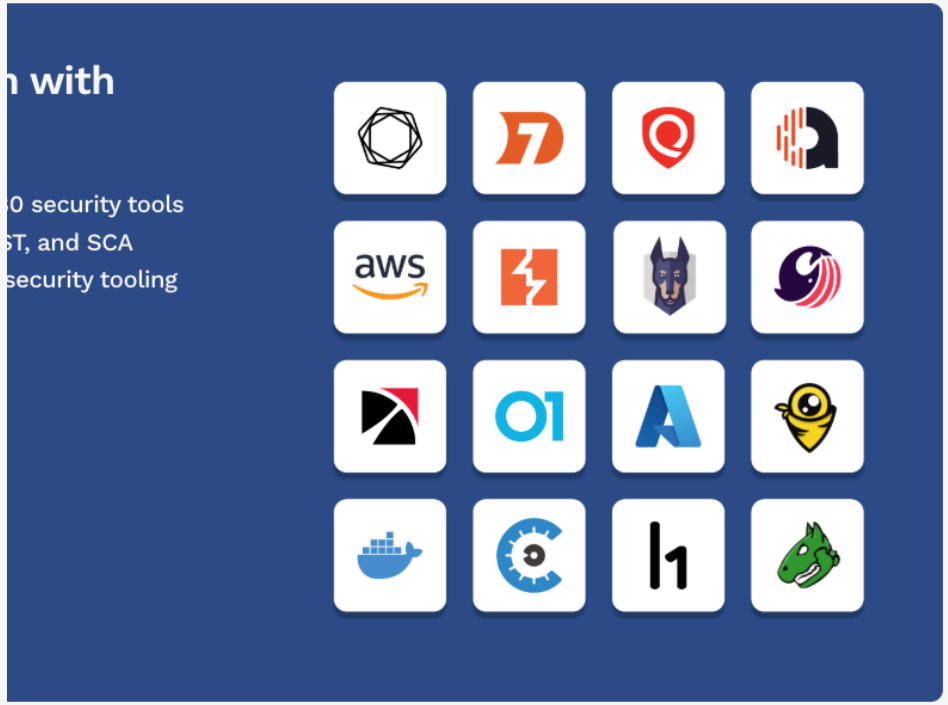
User Access Control
Ensure only authorized access with role-based controls.

Collaboration Tools
Collaborate with features like comments, tasks, and progress tracking.

CVE And CWE Integration
Triage beyond a single finding or endpoint. Inspect by category (CWE).

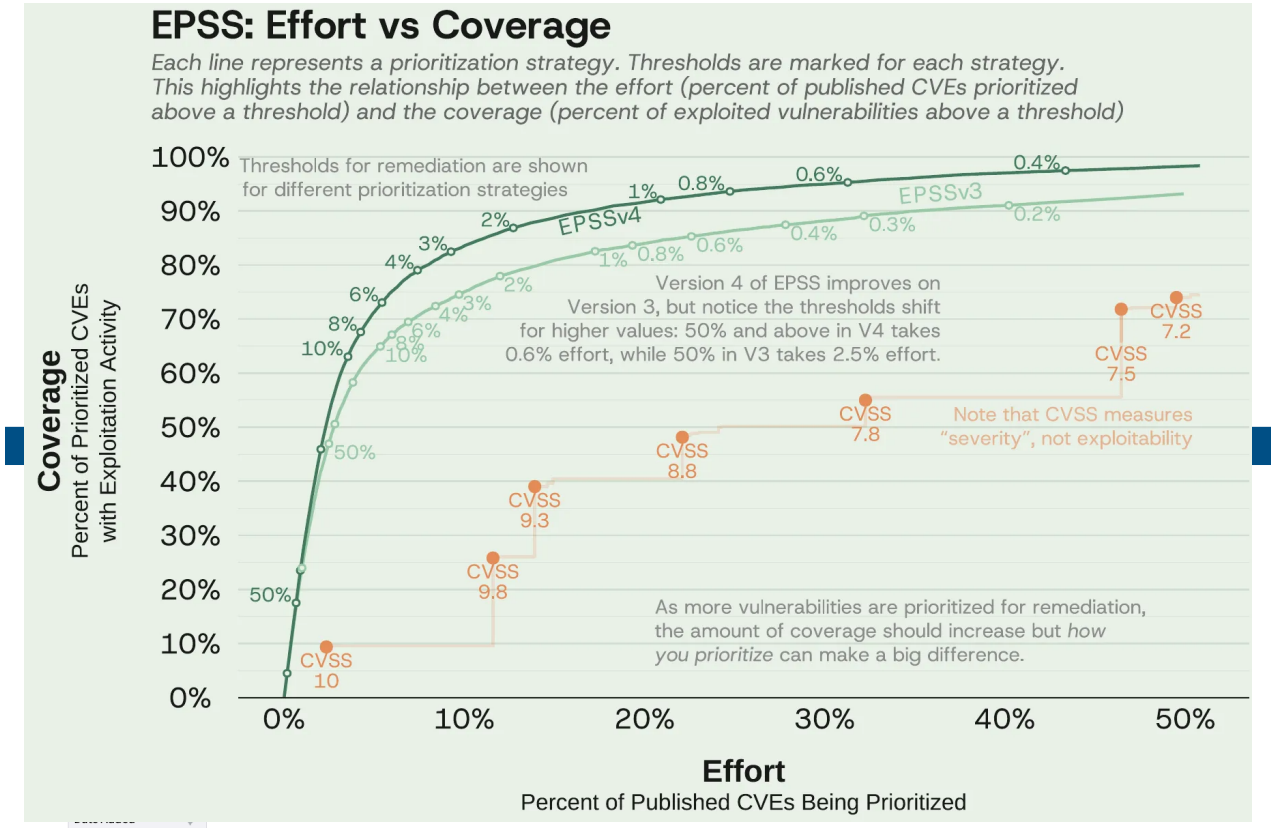
JIRA Integration
Transition from vulnerability detection to remediation with our bi-directional JIRA integration.

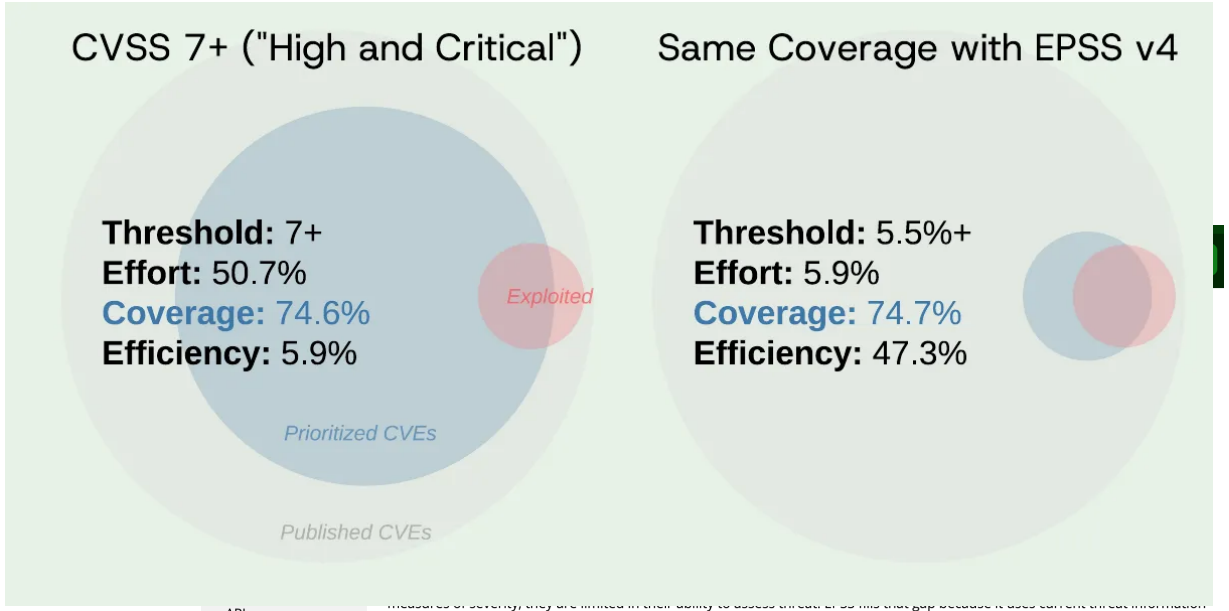
Compliance Reporting
Show compliance with security standards like ASVS.

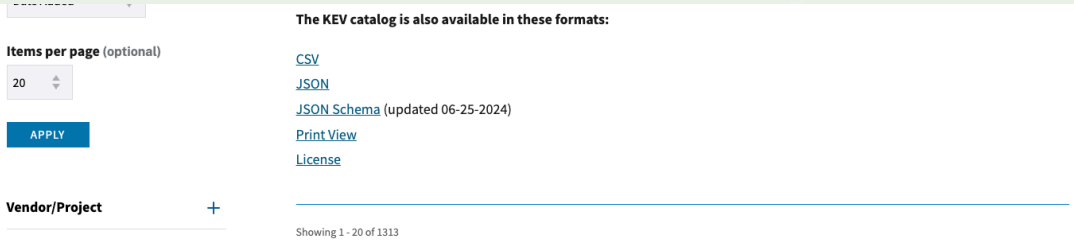


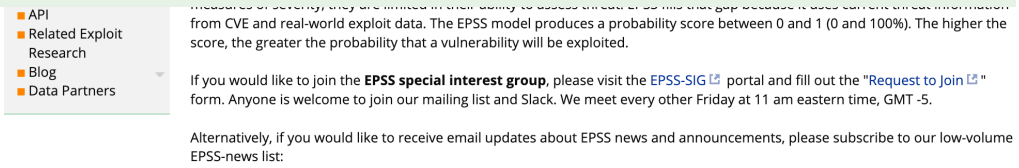
AppSec Results

Use advanced prioritization tools available!


EPSS: Effort vs Coverage
Each line represents a prioritization strategy. Thresholds are marked for each strategy.
This highlights the relationship between the effort (percent of published CVEs prioritized above a threshold) and the coverage (percent of exploited vulnerabilities above a threshold)
Thresholds for remediation are shown for different prioritization strategies
EPSSv4
EPSSv3
Version 4 of EPSS improves on Version 3, but notice the thresholds shift for higher values: 50% and above in V4 takes 0.6% effort, while 50% in V3 takes 2.5% effort.
Note that CVSS measures "severity", not exploitability
As more vulnerabilities are prioritized for remediation, the amount of coverage should increase but how you prioritize can make a big difference.
CVSS 10
CVSS 9.8
CVSS 9.3
CVSS 8.8
CVSS 7.8
CVSS 7.5
CVSS 7.2
Coverage
Percent of Prioritized CVEs with Exploitation Activity
Effort
Percent of Published CVEs Being Prioritized






API
Related Exploit Research
Blog
Data Partners
from CVE and real-world exploit data. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.
If you would like to join the EPSS special interest group, please visit the EPSS-SIG portal and fill out the "Request to Join" form. Anyone is welcome to join our mailing list and Slack. We meet every other Friday at 11 am eastern time, GMT -5.
Alternatively, if you would like to receive email updates about EPSS news and announcements, please subscribe to our low-volume EPSS-news list:

https://www.empiricalsecurity.com/research/epss-effort-vs-coverage

RSAC | 2025 Conference

Software Shelf Life

Medical device & Long term support challenges

Many Voices.
One Community.

Dependency on 3rd party code

BLACKDUCK®

2025 Open Source Security and Risk Analysis Report

Our Findings at a Glance

1,658 projects scanned by Black Duck audits

97% of the codebases contained open source

70% of scanned code had its origin in open source

An average **911** OSS components were found per application

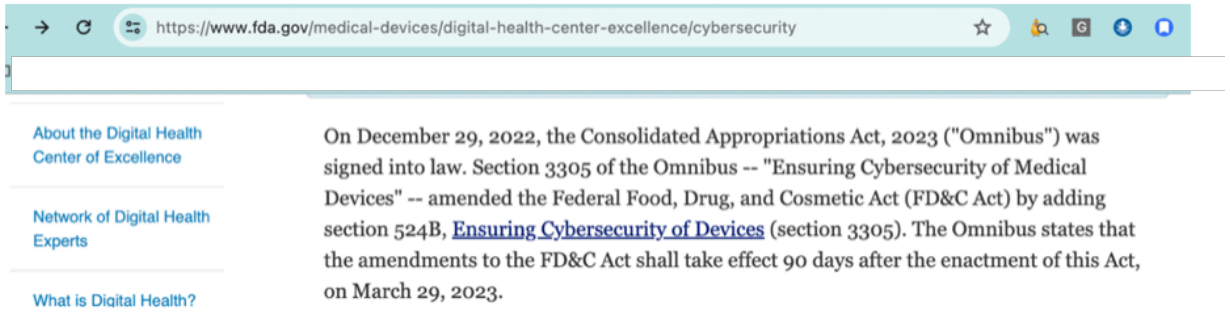
64% of OSS components were transitive dependencies

The number of open source files in an average application has tripled in the last four years.

2020	2022	2024
5,386	11,858	16,082

https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html
https://jfrog.com/whitepaper/the-hidden-cost-of-devsecops-a-developers-time-assessment/

FDA 524B


https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
About the Digital Health Center of Excellence
Network of Digital Health Experts
What is Digital Health?
On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus -- "Ensuring Cybersecurity of Medical Devices" -- amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices (section 3305). The Omnibus states that the amendments to the FD&C Act shall take effect 90 days after the enactment of this Act, on March 29, 2023.

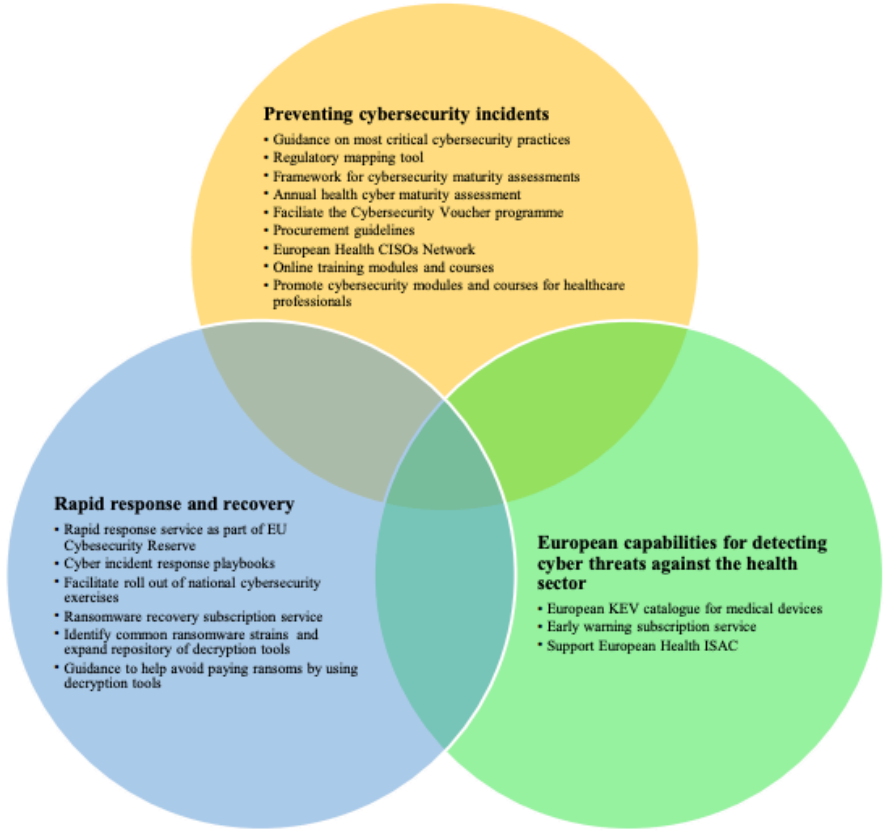
(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;
(2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket update

"(b) CYBERSECURITY REQUIREMENTS.—The sponsor of an application or submission described in subsection (a) shall—
"(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;
"(2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address—
"(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and
"(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;
"(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and
"(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.
"(c) DEFINITION.—In this section, the term 'cyber device' means a device that—
"(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;
"(2) has the ability to connect to the internet; and
"(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.
"(d) EXEMPTION.—The Secretary may identify devices, or categories or types of devices, that are exempt from meeting the cybersecurity requirements established by this section and regulations promulgated pursuant to this section. The Secretary shall publish in the Federal Register, and update, as appropriate, a list of the devices, or categories or types of devices, so identified by the Secretary.".

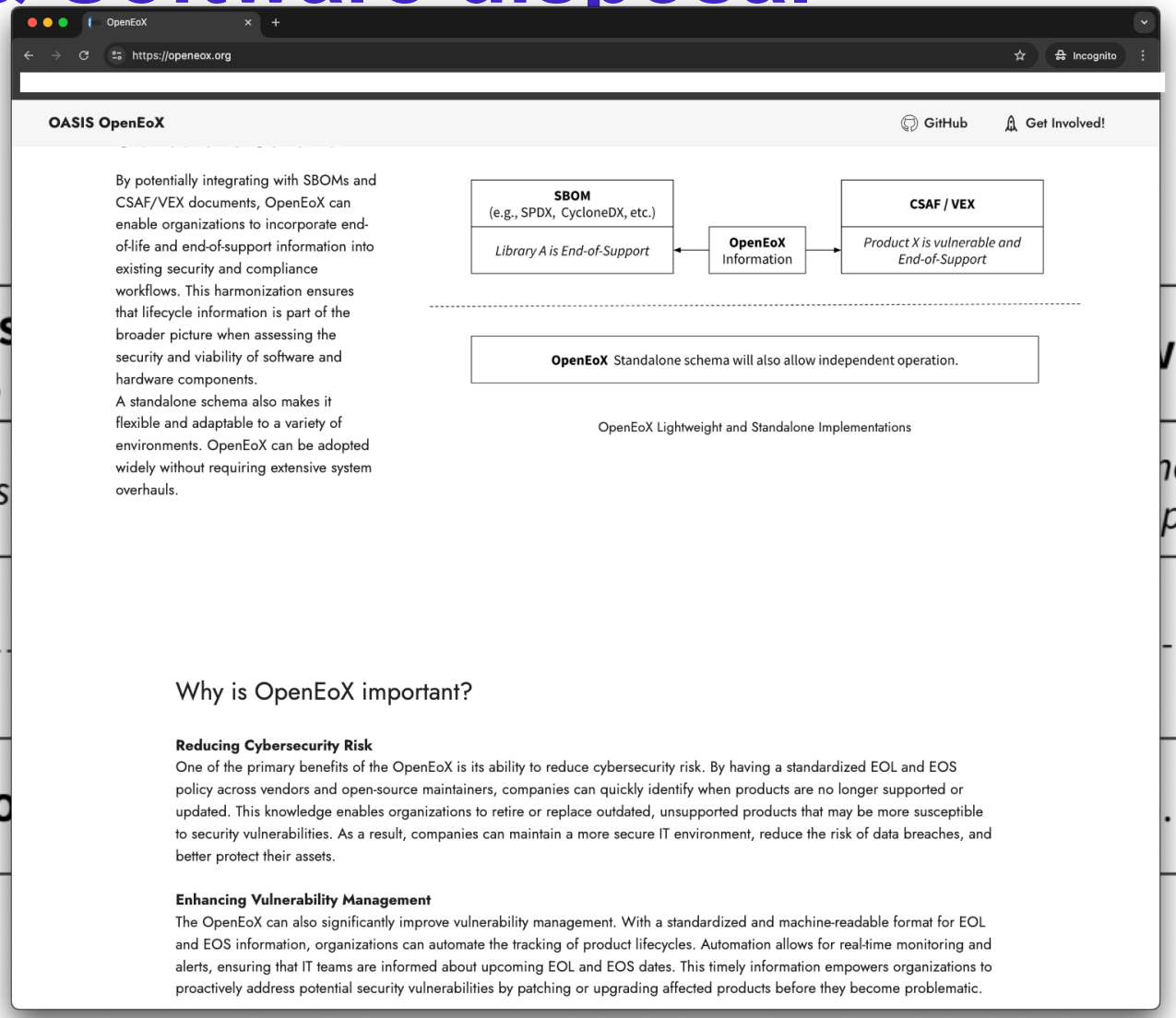
Software Shelf Life

- Medical devices have longer shel
  maintenance is a liability. Longer
  years or so)
- EOX (End of life/End of Support)
  overwhelming with old tool stack.
- MDM space is at the focus of CIS
  EU launching medical device KE
  strategy.ec.europa.eu/en/library/e
  cybersecurity-hospitals-and-healt

Competence Centre (ECCC), will inform further actions at the EU level including the work of the Support Centre.

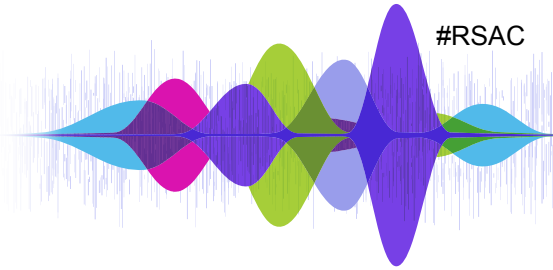

Preventing cybersecurity incidents
• Guidance on most critical cybersecurity practices
• Regulatory mapping tool
• Framework for cybersecurity maturity assessments
• Annual health cyber maturity assessment
• Faciliate the Cybersecurity Voucher programme
• Procurement guidelines
• European Health CISOs Network
• Online training modules and courses
• Promote cybersecurity modules and courses for healthcare professionals
Rapid response and recovery
• Rapid response service as part of EU Cybesecurity Reserve
• Cyber incident response playbooks
• Facilitate roll out of national cybersecurity exercises
• Ransomware recovery subscription service
• Identify common ransomware strains and expand repository of decryption tools
• Guidance to help avoid paying ransoms by using decryption tools
European capabilities for detecting cyber threats against the health sector
• European KEV catalogue for medical devices
• Early warning subscription service
• Support European Health ISAC

OpenEOX & Software disposal


OpenEoX
https://openeox.org
Incognito
OASIS OpenEoX
GitHub
Get Involved!
By potentially integrating with SBOMs and CSAF/VEX documents, OpenEoX can enable organizations to incorporate end-of-life and end-of-support information into existing security and compliance workflows. This harmonization ensures that lifecycle information is part of the broader picture when assessing the security and viability of software and hardware components.
A standalone schema also makes it flexible and adaptable to a variety of environments. OpenEoX can be adopted widely without requiring extensive system overhauls.
SBOM
(e.g., SPDX, CycloneDX, etc.)
Library A is End-of-Support
OpenEoX
Information
CSAF / VEX
Product X is vulnerable and End-of-Support
OpenEoX Standalone schema will also allow independent operation.
OpenEoX Lightweight and Standalone Implementations
Why is OpenEoX important?
Reducing Cybersecurity Risk
One of the primary benefits of the OpenEoX is its ability to reduce cybersecurity risk. By having a standardized EOL and EOS policy across vendors and open-source maintainers, companies can quickly identify when products are no longer supported or updated. This knowledge enables organizations to retire or replace outdated, unsupported products that may be more susceptible to security vulnerabilities. As a result, companies can maintain a more secure IT environment, reduce the risk of data breaches, and better protect their assets.
Enhancing Vulnerability Management
The OpenEoX can also significantly improve vulnerability management. With a standardized and machine-readable format for EOL and EOS information, organizations can automate the tracking of product lifecycles. Automation allows for real-time monitoring and alerts, ensuring that IT teams are informed about upcoming EOL and EOS dates. This timely information empowers organizations to proactively address potential security vulnerabilities by patching or upgrading affected products before they become problematic.

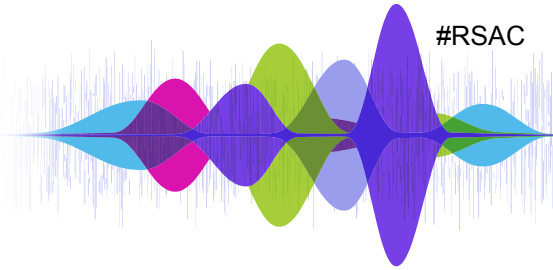
https://openeox.org/

What to Apply in next 90 days



- You can easily deploy an open source ASPM solution!
- Listen all signals coming from source code, whether it is 1st party or 3rd party code (OSS)
- Track defect density (CVE or CWE) per developer/app or product
- Launch company wide SBOM initiative, both for internally developed code and acquired (OTSS) software
- Build and store SBOM with your other artifacts for each commit/branch/ repository/artifact

What to Apply in next 6 months



- Deduplicate & cross reference signals
- Use EPSS as your primary prioritization tool
- Triaging should be done on ASPM, not somewhere else
- Create awareness for Product Security, and align security organization structure to focus on products (https://prods.ec/)
- SBOMs are living documents, store SBOM & maintain them in your ASPM
- Use VEX for issue resolution (justification)
- Adopt Advisory Program, switch using machine readable CSAF format

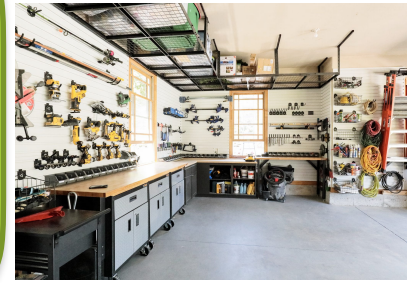
ASPM / GRC Quadrant

Wide ranging

tool & tool stack

ASPM Quadrant

GRC & ASPM Quadrant



Homogeneous

tool & tool stack

Stay in Vendor provided SPM

10 Applications

50+ Applications

RSAC 2025 Conference

Many Voices.
One Community.

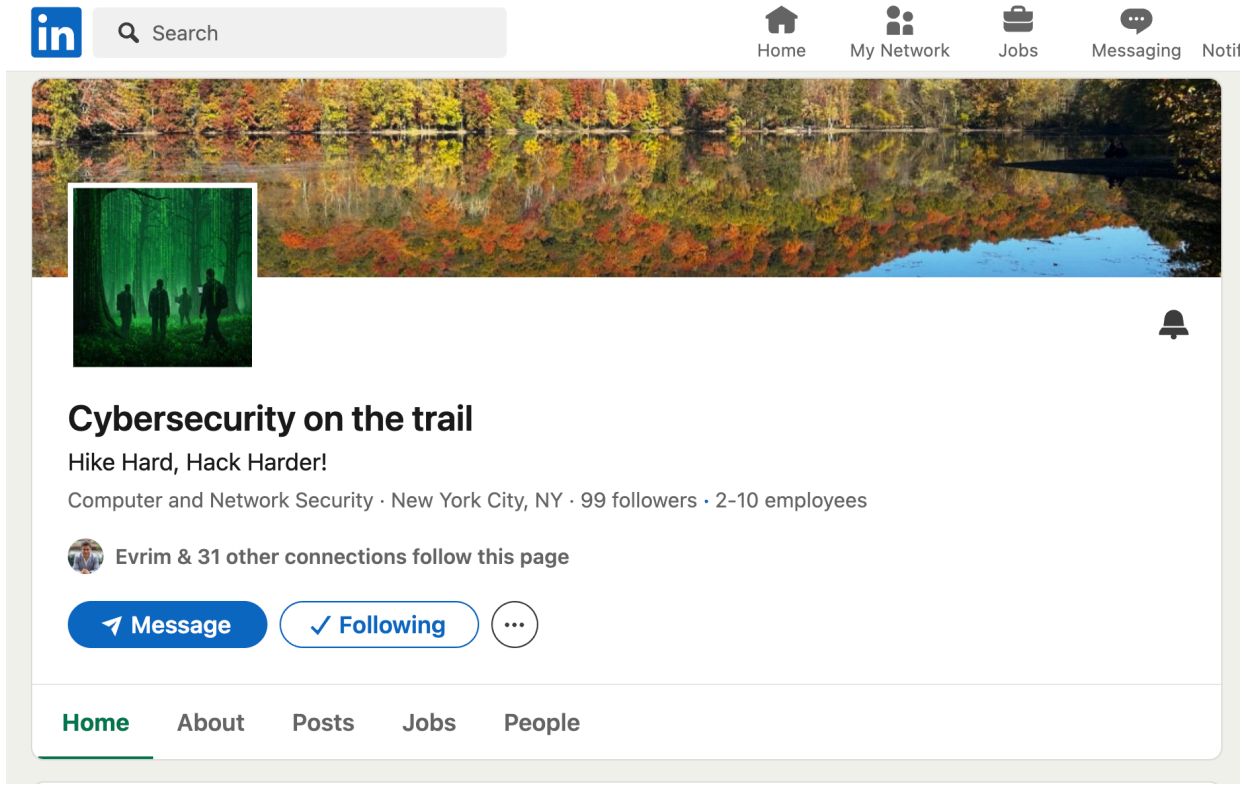
Thank you

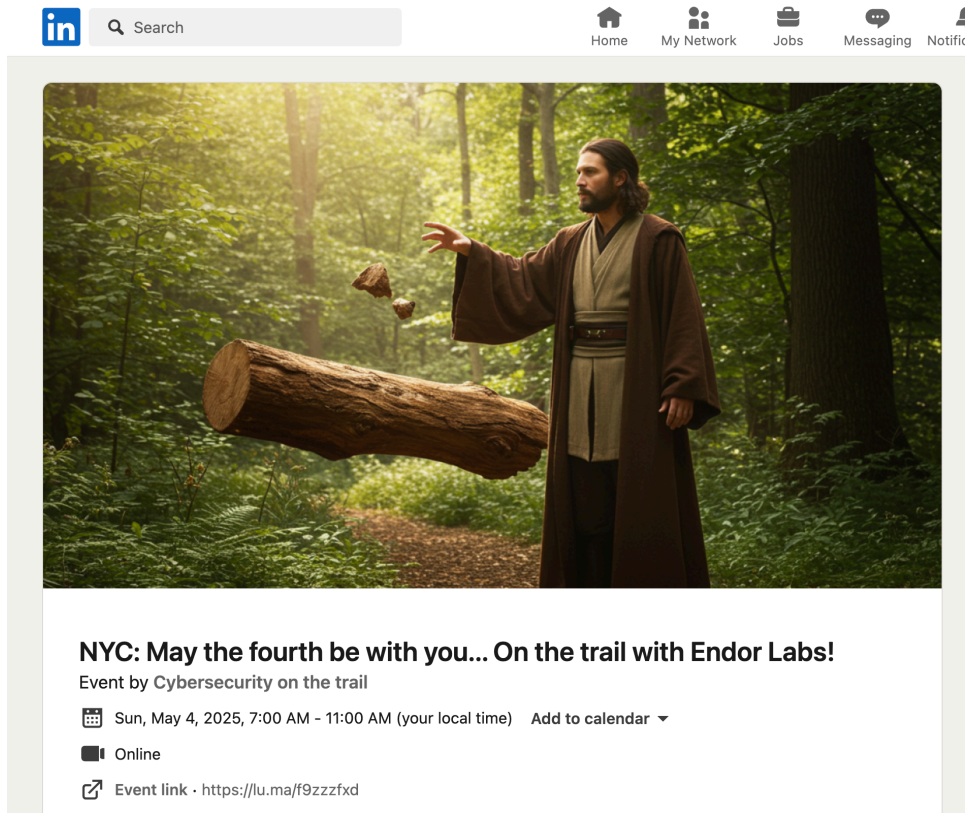
Those who know will always have a job,
those who know why, will be in charge

https://www.linkedin.com/in/kayraotaner

Cybersecurity on the Trail

We are reimagining cybersecurity networking through active and outdoor experiences.




Search
Home
My Network
Jobs
Messaging
NYC: May the fourth be with you... On the trail with Endor Labs!
Event by Cybersecurity on the trail
Sun, May 4, 2025, 7:00 AM - 11:00 AM (your local time)
Add to calendar
Online
Event link · https://lu.ma/f9zzzfxd

"Miss this opportunity, you should not. Grow your skills will. Meet fellow security Padawans you shall. Connections in the Force, important they are." – Master Yoda

- https://www.linkedin.com/company/cybersecurity-on-the-trail

RSAC | 2025 Conference

Bonus slides: Product Security vs Platform Security

Product Security

Adult vs. pediatric hospital: What's the difference?

Why you should choose a pediatric emergency room for your child

Share:

Children are not just "small adults"

"We pediatric surgeons and pediatricians like to say, 'Children are not just small adults,'" says Stephen Megison, M.D., a pediatric surgeon at Children's Health. "Their physiology is different."

For example, there are significant differences between children and adults when it comes to a traumatic injury, which is why it is important to seek care at a Trauma Center that is dedicated to caring for children. Other examples include:

- **A child's heart and vascular system is different than an adult's**. When a child is having a bleeding event, medical staff cannot refer to adult criteria when checking the patient's vital signs — like blood pressure, pulse rate, respiration rate and temperature — because a child's criteria is different. This means they could miss important signs of serious blood loss.
- **There are different injury patterns with fractures**. Because children's bones are more flexible and don't fracture as easily, a fractured bone can cause a much bigger impact on a child's body than an adult's.
- **Smaller children have a bigger head-to-body ratio**. This ratio means young children are more likely to have neck and head injuries than older children and adults. Pediatric ER staff know to look for head and neck injury warning signs specific to children.

CISO vs CPSO

Forbes

INNOVATION

The Rise Of The CPSO: Chief Product Security Officer

By Vince Arneja , Former Forbes Councils Member.
for Forbes Technology Council, COUNCIL POST | Membership (fee-based)

Feb 05, 2021, 08:30am EST

Share Save

Chief Product Officer at GrammaTech, where he leads product strategy for the company's application security testing product portfolio.

GETTY

LOADING VIDEO PLAYER...

FORBES' FEATURED VIDEO

In the past decade, the role of chief information security officer, or CISO, rose to prominence in response to security breaches affecting companies' IT systems, brand reputation, revenues and, in some cases, stock price. Many boards demanded a higher level of focus and accountability for managing cyber security preparedness, threat prevention and response and executive reporting. Recognizing that security has a material impact on their business, the CISO reports directly to the CEO in many organizations. This helps ensure security issues get the board-level attention and are not swept under the rug.